CZASOPISMO BEZPŁATNE ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(89)/2013

ZABEZPIECZENIA

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

artykuł str. 36

W NUMERZE:

- Niemcy już wiedzą, jak lepiej dbać o dane
- Bazy danych osobowych – kupię/sprzedam
- Ile różnych loginów i haseł musisz zapamiętać w pracy?
- Interkom dla każdego! Bezserwerowy system interkomowy Pulse

Platforma wymiany informacji

HID iCLASS SE

Otwarta, elastyczna i doskonale zabezpieczona platforma iCLASS SE®, która ułatwia wszystko.

HID®

iCLASS SE® to kolejna generacja platformy kontroli dostępu HID Global, która umożliwia uwierzytelnianie w różnych komercyjnych technologiach przy użyciu kart bezkontaktowych. Bardzo elastyczna rodzina czytników wraz z szeroką gamą kart zbliżeniowych zapewnia wymianę informacji w różnych środowiskach technologicznych. Technologia iCLASS SE może zostać również użyta w telefonach komórkowych (NFC) i innych urządzeniach inteligentnych. Teraz możesz wykorzystać wszystkie możliwości tej technologii do stworzenia idealnego systemu kontroli dostępu. **Aby uzyskać więcej informacji, odwiedź hidglobal.com/path-Zab**

Spis treści

Wydarzenia, Informacje 4

Monitoring wizyjny

System monitorowania wizyjnego z wykorzystaniem IP – bezpieczeństwo na osiedlu to priorytet
– *Anna Twardowska, Paweł Ruszczyński* 16

Monitoring

STAM-2 – system wspomagania stacji monitorowania
– *Michał Konarski, SATEL* 20

Ochrona peryferyjna

Niewidzialna ochrona domu
– *ATLine* 24

Kontrola dostępu

Nowoczesny budynek bez kluczy
– *Marek Adameczek, Agnieszka Filipowicz* 28

Abloy Protec Cliq – zdalnie programowany system zamknięć od Assa Abloy
– *Grzegorz Korzeniowski, Assa Abloy* 32

Telewizja dozorowa

Grundig CCTV wyłącznie w ofercie C&C Partners Telecom
– *Konrad Staniewski, C&C Partners Telecom* 36

Wysokiej jakości detekcja termowizyjna, PTZ i nadzór HDTV w jednym
– *Agata Majkucińska, Axis Communications* 40

System IP CCTV marki NOVUS dla liczarni pieniędzy i punktów kasowych. Rozdzielczość i czułość kamer IP
– *Patryk Gańko, AAT Holding* 44

SSWiN

Oprogramowanie F-Link dla systemu JABLOTRON 100
– *Piotr Panek, JABLOTRON ALARMS* 48

Systemy zintegrowane

Interkom dla każdego! Bezserwerowy system interkomowy Pulse
– *Adam Gregorczyk, Novatel* 52

Ochrona informacji

Środki bezpieczeństwa fizycznego w ochronie informacji niejawnych (cz. 2)
– *Artur Bogusz, Marek Blim* 58

Publicystyka

Ile różnych loginów i haseł musisz zapamiętać w pracy?
– *Krzysztof Białek* 68

Normalizacja

Niemcy już wiedzą, jak lepiej dbać o dane
– *Paweł Markowski, BOSSG Data Security* 70

Porady prawne

Bazy danych osobowych – kupię/sprzedam
– *Monika Brzozowska* 74

Karty katalogowe 78

Spis teleadresowy 84

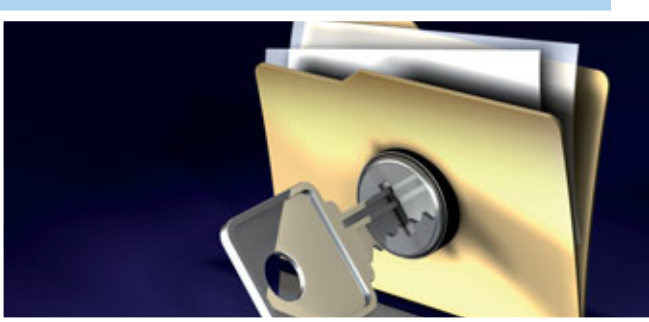
Cennik i spis reklam 94

CZASOPISMO ZABEZPIECZENIA 1/2013

Niewidzialna ochrona domu **24**

Grundig CCTV wyłącznie w ofercie C&C Partners Telecom **36**

Wysokiej jakości detekcja termowizyjna, PTZ i nadzór HDTV w jednym **40**



Środki bezpieczeństwa fizycznego w ochronie informacji niejawnych (cz. 2) **58**

Bosch wprowadza na rynek kamerę stworzoną dla systemów konferencyjnych

Bosch Security Systems wprowadza na rynek nową kamerę kopułkową **HD Conference Dome**, przeznaczoną do pracy w systemach konferencyjnych. Wzbogaca też oprogramowanie systemu konferencyjnego DCN o nową funkcję, która umożliwia jego pełną integrację z tą kamerą.

Nowe rozwiązanie firmy Bosch dla systemów konferencyjnych DCN pozwala na automatyczne sterowanie kamerą HD. Specjalną, dedykowaną do tego celu wersją kamery kopułkowej jest Conference Dome z wyjściem wizyjnym w postaci interfejsu SDI (*Serial Digital Interface*).

Automatyczne sterowanie kamerą zwiększa komfort pracy uczestników konferencji. Pozwala im skupić uwagę na temacie, a także dokładnie zobaczyć zabierającą głos osobę.

Kamera Conference Dome połączona z systemem konferencyjnym DCN śledzi przebieg dyskusji i automatycznie obraca się w kierunku aktualnie przemawiającej osoby. Wizerunek osoby i jej nazwisko wyświetlają się na monitorach lub ekranach projekcyjnych. Kamera zmienia ustawienie po wciśnięciu przycisku mikrofonu na pulpicie konferencyjnym uczestnika lub przewodniczącego konferencji.

Kamera Conference Dome pozwala uzyskać krystalicznie czysty obraz. Jest urządzeniem kompaktowym, niewymagającym chłodzenia i cichym, co umożliwia dyskretną pracę.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Bosch ułatwia dobór głośników

Bosch Security Systems zaktualizował aplikację LSP Select, która pomaga w doborze głośników. Narzędzie jest przeznaczone dla użytkowników IPhone'ów i iPadów.

Optymalny dobór głośników jest zadaniem złożonym, ponieważ instalator musi uwzględnić szereg aspektów, takich jak: parametry akustyczne, sposób montażu, kwestie związane z ochroną środowiska i wymaganymi certyfikatami, jak również dostępność akcesoriów.

Bosch oferuje rozwiązania spełniające wymagania co do dowolnych projektów instalacji akustycznych w obiektach użyteczności publicznej. Zapewnia instalatorom możliwość wyboru urządzenia

Zmiany w ofercie firmy OPTEX

OPTEX Security wprowadza na rynek wiele nowych urządzeń zastępujących dotychczas oferowane czujki ruchu do zastosowań wewnątrz i na zewnątrz budynków oraz bariery podczerwieni. Starsze produkty są stopniowo wycofywane z oferty i zastępowane przez nowoczesne rozwiązania.

Czujki ruchu

- Czujki RX-40QZ/PT zostały wycofane; zastąpiły je czujki RXC-ST.
- Czujki CX-502/502AM zostały wycofane; zastąpiły je czujki serii OPTiMAL – OML-ST/AM (stopień 2 i 3 normy EN 50131). Wiosną 2013 r. ofertę uzupełnią nowe czujki z antymaskingiem serii CDX (stopień 3 normy EN 50131): CDX-AM (PIR 15x15 m) i CDX-NAM (kurtyna PIR 24×2 m).
- Czujki dualne MX-40QZ/PT będą dostępne do końca 2013 r.; zastąpią je czujki RXC-DT – czujkę dualną PIR+MW w identycznej obudowie jak RXC-ST.

Czujki ruchu do zastosowań na zewnątrz budynków

- Czujki VX-402/402R będą dostępne do końca 2013 r.; zastąpi je nowa seria czujek VX INFINITY, do której należą czujki 2x PIR, czujki dualne, czujki z antymaskingiem oraz szeroka gama modeli zasilanych bateryjnie do zastosowania w systemach bezprzewodowych. Nowe czujki VXI będą dostępne latem 2013 r.

Bariery podczerwieni

- Bariery AX-100PLUS/AX200PLUS zostały wycofane; zastąpiły je modele AX-30/70/130TN i AX-100/200TF.
- Bariery AX-250/500PLUS oraz AX-350/650TF będą dostępne do końca 2013 r.; zastąpią je urządzenia serii Smart Line: SL-200/350/650QN i SL-200/350/650QDP – czterowiązkowe bariery podczerwieni o zasięgu 60 m, 100 m i 200 m z modulacją częstotliwości wiązek i czterema kanałami komunikacji (QDP). Będą one dostępne latem 2013 r.

Części zamienne do wycofywanych z oferty czujek zewnętrznych oraz barier podczerwieni, jak np. pokrywy przednie, będą wciąż dostępne u dystrybutorów OPTEX.

Szczegółowe informacje na temat wyrobów znajdują się na stronie *www.optex.com.pl*.

Jacek Wójcik
OPTEX Security

Samsung ulepsza linię sieciowych kamer kopułkowych Full HD

Samsung wprowadził nową serię 3-megapikselowych kopułkowych kamer sieciowych

W modelach z serii 7002 Professional, które są ulepszonymi wersjami wcześniejszych megapikselowych kamer o wysokiej rozdzielczości marki **Samsung** wprowadzono wiele innowacyjnych ulepszeń oraz nowych funkcji.

Wszystkie modele mogą generować obrazy o zróżnicowanej rozdzielczości, od 320×180 do 2048×1536, w tym Full HD 1080p o proporcjach 16:9. Zaawansowana funkcja Wide Dynamic Range (WDR) gwarantuje doskonałą widoczność wszystkich szczegółów, nawet jeśli kadr obejmuje zarówno bardzo jasne, jak i zaciemnione obszary. Natomiast technologia skanowania progresywnego (Progressive Scan) eliminuje rozmycia oraz pozwala na uzyskanie ostrego obrazu ruchomych obiektów i szybko jadących pojazdów.

– *Specyfikacje dla nowej serii 7002 Professional uwzględniają wymagania użytkowników, którzy od kamer wysokiej rozdzielczości oczekują czegoś więcej niż obrazów o jakości dowodowej. Ponadto wychodzą one naprzeciw potrzebom instalatorów* – powiedział **Tim Biddulph**, IP product manager z Samsung Techwin Europe. – *Przykładowo funkcja Simple Focus automatycznie ustawia ostrość kamery. Aby uzyskać optyczne powiększenie obrazu, wystarczy wcisnąć przycisk znajdujący się z tyłu urządzenia. To oczywiście skróci czas instalacji. Jest jednak jeszcze jedna zaleta tej inteligentnej funkcji: przy zmianie trybu z kolorowego na czarno-biały w ramach funkcji dzień/noc Simple Focus automatycznie optymalizuje ustawienie ostrości obrazów.*

Seria 7002 Professional jest kompatybilna z większością wiodących programów służących do zarządzania materiałem wizyjnym (platformami VMS oraz oprogramowaniem do scentralizowanego monitoringu firmy Samsung). Wśród pozostałych funkcji wspólnych dla wszystkich modeli warto wymienić detekcję twarzy oraz detekcję dźwięku przy wykorzystaniu mikrofonu zewnętrznego. Kamery te wyposażono także w system inteligentnej analizy obrazu (IVA) – z funkcjami detekcji ruchu, wykrywania pojawienia się i zniknięcia obiektu, wirtualnej zapory, detekcji przekroczenia granicy chronionego obszaru – oraz w funkcję wyzwalającą alarm w razie nagłej zmiany pola widzenia kamery.

Nowe kamery wytwarzają wiele strumieni wizyjnych przy wykorzystaniu metod kompresji H.264 i MJPEG, dzięki czemu mogą równocześnie służyć do monitoringu w czasie rzeczywistym, monitoringu mobilnego, zapisu obrazów o wysokiej jakości lub efektywnego zapisu na kartach pamięci SD oraz do notyfikacji za pośrednictwem poczty elektronicznej.

– *Wraz z wprowadzeniem serii 7002 Professional oraz atrakcyjnych cenowo kamer megapikselowych i HD z linii LiteNet, udostępnionej na początku bieżącego roku, jesteśmy w stanie zaoferować klientom system nadzoru wizyjnego o wysokiej rozdzielczości dla każdego rodzaju projektu* – powiedział Tim Biddulph. – *Klienci mogą także odnieść korzyści z faktu, że obie serie są kompatybilne z naszym najnowszym sieciowym rejestratorem obrazu SRN-1000, który zaprojektowano z myślą o „modularnym" podejściu do procesu rejestracji i archiwizacji obrazów.*

Nowe modele w serii 7002 Professional:

- SNB-7002 – kamera stacjonarna z wbudowanym mikrofonem,
- SND-7082 – kamera kopułkowa,
- SND-7082F – kopułkowa kamera podtynkowa,
- SNV-7082 – kopułkowa kamera wandaloodporna,
- SNO-7082R – odporna na warunki atmosferyczne kamera pracująca w podczerwieni.

Bezpośr. inf. David Solomons
DRS Marketing

---

z ponad 80 modeli głośników. Stworzył też aplikację LSP Select, pomocną przy doborze najodpowiedniejszego modelu. Zawiera ona innowacyjne narzędzie Loudspeaker Ceiling Tool, za pomocą którego można oszacować liczbę potrzebnych głośników na podstawie wymiarów pomieszczenia i poziomu ciśnienia akustycznego.

Aplikacja, zaprojektowana pierwotnie dla iPhone'ów, jest obecnie dostępna w wersji na tablety iPad. Interfejs użytkownika działa w sposób intuicyjny, uwzględnia wymagania klienta i nie wymaga zaawansowanej wiedzy na temat danych technicznych głośników.

Aplikację LSP Select można pobrać z portalu sklepu internetowego App Store. Więcej informacji na jej temat jest dostępnych na specjalnej, dedykowanej stronie: *www.boschsecurity.com/lspselect*. Można tam znaleźć również bezpośredni link do sklepu.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Bosch Security Systems poszerza możliwości obserwacji w ciemnościach

Całkowita ciemność i odległość dochodząca nawet do 100 metrów nie są już przeszkodą w identyfikacji obiektów. **Bosch Security Systems** zwiększył zasięg oświetlenia w podczerwieni w superszybkich kamerach PTZ serii **MIC 550**.

Kamery serii MIC 550 z promiennikami podczerwieni pozwalają na obserwację terenu na odległość dochodzącą do 150 metrów, i to w warunkach całkowitej ciemności. Z kolei zasięg identyfikacji obiektów wynosi już nawet 100 metrów.

Kamery dualne PTZ o rozdzielczości 550 linii mają zoom optyczny 36x lub 28x, dlatego zapewniają znakomitą czytelność obrazu, niezależnie od odległości obserwowanego obiektu. Bezpośrednio na głowicach kamer zamontowane są dwa trwałe diodowe promienniki podczerwieni emitujące światło o długości fali 850 nm. Umożliwiają one skuteczne dotarcie światła do miejsca, gdzie jest ono potrzebne. Technologia filtra 3D gwarantuje równomierny rozkład oświetlenia pomiędzy pierwszym planem a tłem oraz eliminację problemu powszechnie występującego w przypadku konwencjonalnych promienników podczerwieni, czyli białych plam i niedoświetlenia. Technologia ta pozwala na zachowanie wysokiej jakości obrazu w każdych warunkach oświetleniowych.

Użytkownicy kamer serii MIC 550 mogą śledzić, analizować i wyszukiwać zdarzenia i sceny zarejestrowane w dzień oraz w nocy. Pozwala im na to funkcja inteligentnej analizy obrazu (IVA), realizowana przez kamerę połączoną z siecią IP. Funkcja IVA umożliwia odpowiednie zaprogramowanie kamery i wykrywanie przez nią na przykład obecności osób niepożądanych w 10 wybranych obszarach.

Kamery serii MIC 550 z promiennikami podczerwieni mają aluminiową obudowę z trwałą silikonową wycieraczką oraz osłonę przeciwdeszczową. Ich konstrukcja jest odporna na akty wandalizmu i korozję, dlatego sprawdzają się nawet w trudnym środowisku.

Kamery serii MIC 550 mogą być instalowane w pozycji pionowej, odwróconej lub nachylonej pod kątem 45 stopni, bez konieczności stosowania specjalistycznych zamocowań oraz bez ryzyka obniżenia stopnia ochrony IP.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Nowe kontrolery dostępu do systemu RACS 4

Oferta firmy R**OGER** została poszerzona o dwa nowe kontrolery dostępu o oznaczeniach **PR612** i **PR622**, zgodne stylistycznie z linią wzorniczą Radius. Obydwa urządzenia należą do zaawansowanej serii kontrolerów (serii PRxx2) i funkcjonalnie są odpowiednikami rozpowszechnionego od wielu lat modelu PR302. Kontrolery PR612 i PR622 mogą funkcjonować jako autonomiczne punkty kontroli dostępu lub jako elementy systemu sieciowego RACS 4. Urządzenia mogą być zintegrowane z systemami telewizji dozorowej i centralami alarmowymi, jak również z systemami rejestracji czasu pracy na ogólnych zasadach osiągalnych w ramach systemu RACS 4.

Dane techniczne
- zasilanie 12 V_{DC},
- trzy linie wejściowe,
- wyjście przekaźnikowe 1.5 A/30 V_{DC},
- dwa wyjścia tranzystorowe,
- wbudowany czytnik kart zbliżeniowych EM 125 kHz,
- możliwość dwustronnej kontroli przejścia (wymagany jest dodatkowy czytnik serii PRT),
- 4000 użytkowników,
- bufor 32 000 zdarzeń,
- zegar czasu rzeczywistego,
- współpraca z ekspanderami serii XM-2 i XM-8,
- interfejs komunikacyjny RS485,
- praca w warunkach zewnętrznych.

Więcej informacji na stronie *www.roger.pl.*

Bezpośr. inf. ROGER

Samsung wprowadza bezlicencyjne oprogramowanie do sieciowego nadzoru wizyjnego

Firma **Samsung** wprowadziła na rynek oprogramowanie **Samsung Security Manager** – udostępnianą bez licencji platformę służącą do zarządzania systemami nadzoru wizyjnego. Zaprojektowano ją tak, aby zapewnić klientom jak największe korzyści wynikające z inwestycji w kamery sieciowe, kodery, rejestratory DVR i NVR

Zastosowana w tym rozwiązaniu architektura klient-serwer umożliwia zainstalowanie do 1152 kamer w dowolnej liczbie budynków lub obiektów oraz centralne zarządzanie tymi kamerami, podczas gdy zarejestrowane lub wyświetlane na żywo obrazy z kamer mogą być obserwowane przez autoryzowanych użytkowników z dowolnego miejsca w sieci.

– *Rozwój naszej oferty osiągnął taki etap, że możemy zaproponować klientom kompletny, sieciowy system dozorowy od jednego dostawcy* – mówi **Tim Biddulph**, IP Product Manager w Samsung Techwin Europe. – *Jest więc niezwykle ważne, aby funkcjonalność stworzonego przez nas oprogramowania służącego do zarządzania systemami nadzoru wizyjnego umożliwiała klientom pełne wykorzystanie naszej przełomowej technologii.*

Jedną z najważniejszych funkcji oprogramowania Samsung Security Manager (SSM) jest graficzny interfejs użytkownika. Umożliwia on operatorowi wybór konfiguracji wyświetlania najlepiej dopasowanej do liczby kamer, które musi monitorować jednocześnie. Każda konfiguracja, w której mogą być wykorzystane różne sposoby podziału ekranu o proporcjach 4:3 lub 16:9, może zostać nazwana i zapisana na przyszłość.

Można też zaimportować mapy budynków lub obiektów i nałożyć na nie ikony reprezentujące lokalizacje, w których zainstalowano kamery. Ikony można tak skonfigurować, aby były wyróżniane, gdy pojawi się związany z nimi alarm. Dzięki temu operator może szybko wybierać i monitorować obrazy przekazywane na żywo z kamery znajdującej się najbliżej incydentu, a jednocześnie pozyskać nagranie tego, co mogło się wydarzyć przed wyzwoleniem alarmu. Przeglądarka zdarzeń działająca w czasie rzeczywistym obejmuje dziennik zdarzeń, który może zawierać podgląd jednego kanału oraz komentarze wprowadzane przez operatora. Dziennik zdarzeń sortowanych według numeru kamery lub typu zdarzenia można wyeksportować do formatu XLS lub PDF, a następnie użyć jako dowodu rzeczowego, jeśli będzie to konieczne.

Graficzny interfejs użytkownika SSM sprawia, że rejestrowanie nowych urządzeń jest bardzo proste. Dodatkowo oprogramowanie zapewnia kontrolę stanu systemu i umożliwia automatyczne uaktualnianie dowolnego urządzenia firmy Samsung dostępnego w sieci.

– *SSM to doskonały przykład tego, że firma Samsung skupia się na tym, co ważne dla naszych klientów* – mówi Tim Biddulph. – *Rozwiązanie SSM zastąpi nasze oprogramowanie Net-i Viewer. Jest udostępniane bez licencji i zawiera przydatne funkcje, takie jak pełne rejestrowanie aktywności, zwykle będące częścią komercyjnego oprogramowania do zarządzania materiałami wizyjnymi.*

Bezpośr. inf. David Solomons
DRS Marketing

WŁODZIMIERZ KUCZKOWSKI

Włodka pożegnaliśmy 10 stycznia 2013 roku na Powązkach w Warszawie.

Odszedł od nas niespodziewanie, w pierwszym dniu nowego roku. Wspominamy Go jako wspaniałego człowieka, przyjaciela wielu z nas, wybitnego działacza naszego Stowarzyszenia.

Ostatni raz spotkaliśmy się z nim na IX Zjeździe Sprawozdawczo-Wyborczym 16 listopada 2012 roku, kiedy to otwierał zjazd jako przewodniczący rady Stowarzyszenia, a potem na sesji poświęconej XX-leciu Stowarzyszenia wręczał diamentowe i złote Honorowe Odznaki Stowarzyszenia „POLALARM" swoim kolegom.

Był wybitnie zasłużony dla rozwoju technicznej ochrony osób i mienia w Polsce oraz dla ruchu społeczno-zawodowego. Uznanie dla Jego działalności potwierdzały przyznane Mu przez Stowarzyszenie nagrody Orła Rozwoju, Złotego Pioniera Rozwoju Technicznej Ochrony w Polsce. Serdecznie Mu dziękujemy za olbrzymi wkład pracy w działalność Stowarzyszenia, a zwłaszcza za:

– prowadzenie, od początku, ogólnopolskiego konkursu „Polski Mistrz Techniki Alarmowej" – jako przewodniczący,
– wieloletnie członkostwo w Komisji Specjalizacji Zawodowej Inżynierów i Techników,
– kierowanie, od dwóch kadencji, radą Stowarzyszenia jako przewodniczący,
– współudział w zorganizowaniu Mazowieckiego Przedstawicielstwa Stowarzyszenia i kierowanie nim jako prezes zarządu.

Za tę rozległą działalność w „POLALARM" Włodek otrzymał także inne wyróżnienia, m. in. Złotą Honorową Odznakę NOT, Złotą Honorową Odznakę KIG oraz – od prezydenta Polski – Srebrny Krzyż Zasługi.

Nasz serdeczny Kolega i Przyjaciel na zawsze pozostanie w naszej pamięci i w naszych sercach jako wspaniała postać, wzór godny naśladowania.

Cześć Jego pamięci!

Bezpośr. inf. POLALARM

WŁODZIMIERZ KUCZKOWSKI

należał do Stowarzyszenia „POLALARM" od 1993 roku, był rzeczoznawcą.

W Stowarzyszeniu pełnił funkcje:
– przewodniczącego komisji konkursowej „Polski Mistrz Techniki Alarmowej",
– przewodniczącego rady Stowarzyszenia,
– prezesa zarządu Mazowieckiego Przedstawicielstwa „POLALARM".

Bosch wspiera projektantów systemów sygnalizacji pożarowej

Eksperci Bosch Security Systems po raz kolejny współprowadzili szkolenie CNBOP

Na początku listopada w Centrum Naukowo-Badawczym Ochrony Przeciwpożarowej (**CNBOP**) odbyła się kolejna edycja szkolenia dla projektantów, instalatorów i konserwatorów systemów sygnalizacji pożarowej. Wzięło w niej udział ponad czterdzieści osób.

Szkolenia w tej formule są organizowane przez CNBOP od około pięciu lat i kierowane do osób świadczących usługi w obszarze zabezpieczeń przeciwpożarowych. Szkolenie trwa cztery dni i składa się z wykładów, których tematyka obejmuje aspekty prawne, wytyczne projektowania, instalowania i konserwacji systemów oraz warsztatów praktycznych. Podczas części praktycznej uczestnicy mogą zobaczyć, jak wygląda programowanie centrali; chętni mogą ją też samodzielnie zaprogramować. Szkolenie kończy egzamin, a jego pozytywny wynik uprawnia do otrzymania certyfikatu kwalifikacji.

Wśród prowadzących szkolenie byli eksperci ze Szkoły Głównej Służby Pożarniczej, z Komendy Głównej Państwowej Straży Pożarnej i z firmy Bosch.

– Na tegorocznym szkoleniu zaprezentowaliśmy jedno z narzędzi wspierających projektantów w przygotowaniu projektów i wycen – program Planning Tool. Uczestnicy mieli możliwość zapoznania się z narzędziem również na warsztatach praktycznych, gdzie w ramach ćwiczeń przygotowywali w grupach opis projektu, wycenę, schemat blokowy, dzięki czemu mogli sami przekonać się, jaką rolę narzędzie to może odegrać w ich codziennej pracy – mówi **Monika Kołodziejczyk** z **Bosch Security Systems**.

W tym roku, na Międzynarodowych Targach Ochrony Pracy, Pożarnictwa i Ratownictwa SAWO, CNBOP otrzymał Złoty Medal SAWO w kategorii edukacji i prewencji za szkolenia dla projektantów, instalatorów i konserwatorów systemów sy-

Zdalny nadzór wizyjny HD tylko z Bosch Security Systems

Bosch wprowadza aplikację Video Security na iPady

Bosch wprowadza nowy standard w wizyjnych systemach dozorowych HD. Obecnie, dzięki wykorzystaniu aplikacji na iPady, można obserwować obiekt z dowolnego miejsca na kuli ziemskiej i o każdej porze.

Nowa aplikacja – Video Security na iPady – wykorzystuje technologię dynamicznego transkodowania (*Dynamic Transcoding Technology*) i zapewnia dostęp do kamer wizyjnego systemu dozorowego nawet przy niskiej przepustowości łącza internetowego. Dzięki temu w każdej chwili można sprawdzić, co w określonym momencie widzi kamera.

Aplikacja współpracuje z dowolnymi kamerami Bosch H.264 SD/HD. Pozwala na sterowanie kamerami PTZ, zmianę ich azymutu i nachylenia oraz przybliżenie i regulację ostrości obrazu. Ma także funkcję odtwarzania z intuicyjną obsługą za pomocą pokrętła szybkiego wyboru, osią czasu ze zintegrowaną listą alarmów i podglądem w formie miniaturek obrazów z kamer. Obsługuje też funkcję wyszukiwania materiałów dowodowych, dostępną w technologii inteligentnej analizy obrazu (IVA – *Intelligent Video Analysis*), pozwalającą na wychwycenie obiektów przekraczających zdefiniowane linie graniczne oraz wykrycie ruchu w określonym obszarze i przedziale czasowym. Umożliwia również dalsze przetwarzanie zarejestrowanych materiałów poprzez przesyłanie zrzutów ekranowych e-mailem lub zapisywanie ich w bibliotece zdjęć, a także eksportowanie nagrań na serwery FTP lub do serwisów typu Dropbox bazujących na technologii chmury.

Aplikacja Video Security rozszerza możliwości najnowszej linii transkoderów Bosch VideoJet XTC lub VideoJet X20/X40 XF z oprogramowaniem 5.60 lub nowszym i jest dostępna w sklepie App Store. Więcej informacji na ten temat można znaleźć na stronie *www.boschsecurity.com.*

Aby zapewnić najwyższy standard bezpieczeństwa, aplikacja jest chroniona hasłem dostępu oraz oferuje bezpieczne, szyfrowane połączenie SSL pomiędzy nią a transkoderem.

– *Dzięki wprowadzeniu funkcji zdalnej obsługi Bosch pierwszy na rynku zapewnia natychmiastowy dostęp do wizyjnych systemów dozorowych HD. Nowa aplikacja, w połączeniu z rozwiązaniami sprzętowymi, otwiera przed użytkownikami niedostępne do tej pory możliwości* – zapewnia Radomir Dębek, Product Manager Bosch Security Systems.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

gnalizacji pożarowej. Nagrodę przyznał Minister Pracy i Polityki Społecznej.

Współpraca z firmami projektowymi i indywidualnymi projektantami systemów bezpieczeństwa należy do kluczowych zadań Bosch Security Systems. Projektanci mogą liczyć na szeroki zakres doradztwa technicznego, począwszy od etapu koncepcji, aż do fazy wykonawczej projektu. Bosch od lat zwraca uwagę na proces przekazywania wiedzy projektantom i firmom partnerskim, tak aby ułatwić im wykorzystywanie najnowszych rozwiązań przy tworzeniu koncepcji zabezpieczenia obiektów. Oprócz szkoleń i doradztwa technicznego Bosch oferuje także darmowy dostęp do aktualnych materiałów ułatwiających prace projektowe. Wszystkim zainteresowanym projektantom polecamy wizytę na stronie internetowej *www.boschsecuritysystems.pl*, gdzie znajdują się przydatne narzędzia projektowe dla każdej grupy produktów z oferty firmy Bosch.

Bezpośr. inf. Katarzyna Staroń
Robert Bosch

Made in Sweden

Axis Partner Conference Polska

Jak wiadomo, siła przedsiębiorstwa zależy w dużej mierze od osiągania dobrych wyników sprzedaży. **Axis Communications** jest producentem urządzeń do sieciowych systemów wizyjnych. Pozycja firmy zależy od wielu czynników, ale jednym z ważniejszych jest działanie dobrze rozwiniętej sieci lojalnych światowych partnerów. Nagrodą dla tych najlepszych są coroczne wyjazdy „motywacyjne". Mają one zachęcać do dalszej wytężonej pracy i do poprawy wyników sprzedaży. Organizatorzy Axis Partner Conference Polska, tradycyjnie już, wykonali zadanie na szóstkę, dlatego spotkanie to zapewne zapadnie w pamięć uczestników.

Na „wyprawę życia" (te słowa słyszałam wielokrotnie) wyjechało ośmiu przedstawicieli polskich firm oraz dwie przedstawicielki prasy branżowej. Przed przejściem do relacji opiszę w wielkim skrócie wydarzenia, które miały miejsce, zanim dotarliśmy do celu naszej podróży – do Jukkasjärvi k/Kiruny.

10 grudnia 2012 roku z lotniska Chopina w Warszawie udaliśmy się wraz **Agatą Majkucińską**, przedstawicielką firmy Axis (Key Account Manager Poland), do Kopenhagi, skąd pojechaliśmy do Lund – mostem Øresundsbron (najdłuższym mostem na świecie), gdzie znajduje się siedziba firmy. Na miejscu czekali na nas przedstawiciele Axisa. Po krótkim powitaniu współzałożyciel i członek zarządu firmy **Martin Gren**, w asyście **Petra Tosnera** (Marketing Manager Region EE), **Agaty Majkucińskiej** i **Iriny Kälberg Rönning**, wręczył pamiątkowe statuetki i dyplomy.

Przyznano nagrody w następujących kategoriach:
- najbardziej lojalny partner w 2012 roku,
- innowacje w polskim sektorze edukacyjnym,
- największy projekt w 2012 roku,
- partner z największym potencjałem w 2012 roku,
- najbardziej innowacyjny projekt systemu monitoringu miejskiego w 2012 roku,
- najlepsze wyniki ekonomiczne w 2012 roku.

Martin Gren przedstawił historię i trendy technologicznego rozwoju telewizji sieciowej. Przypomniał, że gdy firma zaczynała

AXIS COMMUNICATIONS w pigułce

Firma Axis powstała w 1984 roku. Początkowo założyciele zajmowali się usługami na szwedzkim rynku IT. We wczesnych latach 90. rozszerzyli swoją działalność i wprowadzili na rynek sieciowe serwery do drukarek umożliwiające wykorzystanie protokołu TCP/IP w obsłudze drukarek w raczkujących biurowych sieciach LAN. Firma Axis stała się światowym liderem w dziedzinie podłączania do sieci drukarek IBM, a następnie w dziedzinie wydruku poprzez sieć.

Założenia przyjęte w 1984 były konsekwentnie przestrzegane i – podobnie jak w przypadku drukarek – we wczesnych latach 90. firma stała się światowym liderem w dziedzinie kamer sieciowych i serwerów do kamer analogowych. Kiedyś drukarki IBM miały tylko standardowy interfejs równoległy, taki jak większość drukarek na całym świecie. Pod koniec lat 80. Axis wyprodukował serwer do drukarki, który umożliwiał podłączenie dowolnej drukarki do sieci, a w latach 90. wyprodukował serwer do kamery umożliwiający podłączenie analogowej kamery do sieci. Można powiedzieć, że w tamtym okresie (i jeszcze długo później) nikt na świecie nie zajmował się tym, więc Axis rzeczywiście był liderem i pionierem w tej dziedzinie.

W późnych latach 90. firma próbowała tworzyć sieciowe serwery do różnych urządzeń, czyli szukać takich miejsc, w których są jakieś urządzenia pracujące niezależnie od siebie, które można podłączyć do sieci. Dzięki temu pojawił się pomysł podłączania kamer do sieci. Rozwijając koncepcję łączenia wszystkiego, czego się tylko da, w sieć Axis wyprodukował pierwszą na świecie kamerę sieciową AXIS 200. Było to niewątpliwie bardzo duże osiągnięcie, bo konkurencja w ogóle się tym nie zajmowała. Axis wyprzedził inne firmy co najmniej o kilka lat i można powiedzieć, że wyznaczył nowe trendy. Pierwsza kamera została szybko udoskonalona. Posłużono się własnymi, opracowanymi specjalnie w tym celu układami scalonymi, wytwarzanymi w technologii ASIC. Przedstawiciele firmy Axis podkreślają, że drugim czynnikiem, który zadecydował o światowym sukcesie, było utrzymanie raz przyjętych założeń dotyczących systemu dystrybucji produktów, co ich zdaniem zrewolucjonizowało ówczesny światowy rynek CCTV.

Lata 1998–2002 to kierowanie się przyjętymi założeniami, które umożliwiły konsekwentny rozwój. Powstała kamera AXIS 2100, która zdominowała rynek na kolejne pięć lat. Po roku 2000 Axis odnotował spadek sprzedaży serwerów do drukarek i skoncentrował się na kamerach. Rozwinięto sieć światowych biur firmy oraz podjęto duże inwestycje.

W dziedzinie wizyjnych systemów dozorowych zapoczątkowano proces stopniowego zastępowania systemów analogowych cyfrowymi, który trwa nadal. Opracowano program rozwoju, który jest nadal realizowany. Poszczególne etapy to: 2004 – pierwsza kamera z zasilaniem PoE, 2004 – zastosowanie przetwornika CMOS w miejsce CCD, 2004 – zastosowanie rozdzielczości HDTV, 2008 – zastosowanie kompresji H.264, 2008 – opracowanie kamer HDTV zgodnych z zaleceniami SMTPE (światowego zrzeszenia specjalistów z dziedziny telewizji), 2010 – wprowadzenie na rynek sieciowych kamer termowizyjnych, 2011 – wprowadzenie na rynek sieciowych kamer termowizyjnych, 2011 – wprowadzenie nowych technologii poprawiających jakość obrazu (*Lihgtfinder*), 2011 i później – skoncentrowanie się na sprzęcie pracującym zgodnie ze standardem HDTV (tylko Axis używa określenia HDTV – konkurencja mówi o kamerach HD, Full HD etc.).

Od 2010 roku firma Axis produkuje sprzęt, który można stosować wraz ze zgodnymi ze światowymi standardami rozwiązaniami innych producentów, dzięki czemu otworzyła się na cały światowy rynek, a jej produkty znajdują bardzo wiele zastosowań w bardzo różnych dziedzinach. Firma Axis postawiła na kontakt z klientami i stara się ułatwiać im pracę – organizuje szkolenia, prezentacje, warsztaty itp. Ustala potrzeby i stara się wychodzić im naprzeciw – nie próbuje generować popytu, ale raczej dostosować się niego.

swoją działalność, królowała telewizja analogowa. Obecnie to IP zaczyna dominować, a – jak słusznie zauważył – firma Axis była pierwsza i nadal mocno się trzyma. Produkcja własnego procesora do obróbki obrazu daje Axisowi dużą przewagę nad konkurencją (obecnie, wg IMS Research, Axis zajmuje pierwsze miejsce na rynku kamer dozorowych). Tanieją komponenty, takie jak pamięci czy mikroprocesory. Generalnie jest tendencja do tworzenia kamer wyposażonych w procesory o dużej mocy obliczeniowej i pojemnej pamięci, które realizują złożone funkcje alarmowe, np. funkcje wykrywania i identyfikacji obiektów. Axis ma ambicje tworzyć nowe i niespotykane rzeczy. Jest to możliwe dzięki wdrażaniu nowych technologii opracowywanych przez firmę. Przykładem może być bardzo mała kamera o wysokiej rozdzielczości. Bardzo silną stroną Axisa są kamery termowizyjne,

które powoli zdobywają rynek urządzeń termodetekcyjnych. Axis tworzy prognozy i prowadzi badania rynku. Wynika z nich, że nawet w małych systemach dozorowych zaczyna się stosować technologię sieciową, a do 2016 roku zdecydowanie wzrośnie sprzedaż kamer sieciowych. Axis promuje kamery HDTV. Każdy, kto ma w domu nowoczesny telewizor, będzie mógł przeglądać obrazy z kamer w standardzie HDTV. Zadowoleni będą również fachowcy z branży.

Martin Gren oprowadził nas po **Axis Experience Center**. Następnie **Petra Bennermark** (Produkt Manager, Video) zapoznała nas z produktami i technologiami rozwijanymi przez firmę Axis. Przypomniała o produktach, które pojawiły się w roku 2012, oraz poinformowała o nowościach, które mają ukazać się na początku 2013 roku. Mieliśmy też okazję zwiedzić **Axis Configuration & Logistics Center**. Naszym przewodnikiem był **Johan Stjernfelt** (Supervisor CLC1), który poinformował nas o procesach jakościowych i sposobach eliminacji pomyłek podczas produkcji i wysyłki urządzeń do klientów. **Petr Tosner** przedstawił plany marketingowe dla regionu EE, zaprezentował biura w Pradze czeskiej i w Moskwie (przedstawił strukturę organizacyjną swojego biura), wskazał na jeszcze większe możliwości współpracy z polskimi partnerami, a także ogłosił konkurs *case study* (do wygrania jest pięć iPhone'ów 5).

Pierwszy wieczór spędziliśmy w restauracji Rådhuskällaren. Jest to jedna z najstarszych i najbardziej szanowanych restauracji, znana z nienagannej obsługi i wyjątkowej atmosfery.

Serwuje się tam pyszne dania kuchni szwedzkiej. Lokal mieści się w piwnicy ratusza w Malmö. Wyjątkowa atmosfera i przedświąteczny nastrój udzieliły się wszystkim.

Następnego dnia – 11 grudnia – polecieliśmy do Kiruny – miasta w północnej Szwecji, największego w krainie Laponii i najbardziej wysuniętego na północ kraju. Prosto z lotniska, w specjalnie przygotowanej dla nas odzieży, na sankach ciągniętych przez psy, udaliśmy się do Jukkasjärvi (ok. 18 km od Kiruny) – lapońskiej wioski leżącej 200 km od koła podbiegunowego. Znajduje się tam duma Szwecji – uznawany przez przewodników z całego świata za wyjątkową atrakcję turystyczną ICEHOTEL. Hotel ten jest zbudowany, a raczej budowany, z ogromnych brył śniegu i lodu z zamarzniętej rzeki Torne (jednej z najczystszych w Europie), które wiosną każdego roku najzwyczajniej rozpuszczają się i spływają do rzeki. Hotel jest budowany co roku na nowo i za każdym razem przybiera inny kształt, wyczarowywany przez artystów z całego świata. Każdy pokój jest inny, wykonywany przez innego artystę. We wnętrzach dominuje biel i błękit. Ściany są zdobione










rzeźbieniami, chętnie wykorzystuje się rozmaite instalacje świetlne, a w korytarzach są galerie lodowych rzeźb. Na terenie hotelu jest też Absolut ICEBAR, gdzie kolorowe drinki podawane są w szklankach wykonanych z lodu, a ich nazwy są takie same jak nazwy poszczególnych pokoi hotelowych. Posiłki również podawane są w lodowych naczyniach.

Mieliśmy okazję spędzić noc w tym baśniowym hotelu. Oczywiście była możliwość wybrania noclegu w ciepłym, „zwykłym" hotelu, ale nikt z niej nie skorzystał. Wszyscy byliśmy ciekawi nocy na lodowym łożu, okrytym jedynie skórami reniferów, w temperaturze -5°C (temperatura na zewnątrz: -35°C). Dostaliśmy śpiwory termiczne, a rano podano nam gorący napój z borówek. W tym roku byliśmy pierwszymi lokatorami tego hotelu, który był jeszcze tworzony. Gdy wyjeżdżaliśmy, otrzymaliśmy pamiątkowe certyfikaty potwierdzające spędzenie w nim nocy.

Wspaniałą atrakcją była możliwość zobaczenia zorzy polarnej. Nasi koledzy, nie bacząc na niską temperaturę i głęboki śnieg, opuścili wioskę i udali się tam, gdzie była najlepiej widoczna. Udało im się zrobić wiele ciekawych fotografii. Zorza pokazała się chyba specjalnie dla nas, bo ani kilka tygodni wcześniej, ani później nie była widoczna.

Trzeciego dnia, 12 grudnia, **Agata Majkucińska** podczas krótkiej konferencji przekazała nam najważniejsze informacje dotyczące działalności firmy Axis. Podkreśliła raz jeszcze, że podstawą jest światowa sieć partnerów, duży asortyment oferowanych urządzeń, a także światowy zasięg. Wypełniliśmy specjalnie przygotowaną ankietę, która miała na celu zasięgnięcie informacji dotyczących między innymi oczekiwań partnerów firmy, zadowolenia klientów i oferty.

Zaraz po tym spotkaniu udaliśmy się na przejażdżkę po okolicy. Do dyspozycji mieliśmy śnieżne skutery. Przejeżdżaliśmy przez












ośnieżony las i zamarzniętą rzekę, więc mieliśmy okazję podziwiać piękną okolicę. Podczas kolacji mogliśmy podzielić się wrażeniami z pobytu w Szwecji. Wszyscy zgodnie stwierdzili, że pomysł na zorganizowanie wyjazdu w okolice koła podbiegunowego był strzałem w dziesiątkę. Mieliśmy okazję ugruntować lub uzupełnić swoją wiedzę dotyczącą oferty firmy Axis i dowiedzieć się o jej planach na przyszłość, a forma spotkania była wyjątkowo atrakcyjna.

Partnerzy firmy Axis cenią ją za produkty, które wyznaczają światowe trendy, stabilność, dużą dynamikę rozwoju, wzorową organizację pracy, konsekwencję w działaniu, dbałość o klienta, silne wsparcie techniczne oraz ciągłe edukowanie swoich klientów – na szkoleniach i warsztatach, poprzez udostępnianie materiałów szkoleniowych, samouczków i przewodników. Oprócz kamer i serwerów sieciowych firma Axis produkuje wiele akcesoriów. Ponadto udostępnia bezpłatny system AXIS Camera Companion, który służy do zarządzania materiałem wizyjnym i znajduje zastosowanie w małych instalacjach zawierających od kilku do kilkunastu kamer, a także bezpłatne oprogramowanie narzędziowe AXIS Camera Companion Buyers' Tool, dostępne dla wszystkich nabywców kamer Axis. Oprogramowanie to pozwala na łatwy dobór liczby i rodzaju kamer Axis niezbędnych do budowy systemów dozorowych spełniających wymagania użytkowników końcowych, a także umożliwia dobór sprzętu sieciowego i innych składników niezbędnych do zbudowania instalacji zawierających określoną liczbę kamer. Dla wielu klientów nie bez znaczenia jest również pochodzenie towaru – urządzenia firmy Axis są produkowane w Szwecji.

Opracowała Teresa Karczmarzyk

Zapraszamy do obejrzenia fotorelacji *www.zabezpieczenia.com.pl.*

Bezpieczeństwo na osiedlu to priorytet

System monitorowania wizyjnego z wykorzystaniem IP

Anna Twardowska
Paweł Ruszczyński

Rośnie w Polsce liczba osiedli mieszkaniowych, na których instalowane są systemy monitoringu wizyjnego. Niektóre nowobudowane osiedla od razu wyposażane są w takie systemy. Jest to dodatkowy czynnik zachęcający potencjalnych nabywców do kupna lokali. Jeśli zamierzamy wyposażyć w taki system osiedle już istniejące, to musimy wcześniej zapoznać się z oczekiwaniami przyszłych użytkowników. Ułatwi to wybranie kamer i sposobu ich rozmieszczenia, a także wybór odpowiedniego rejestratora. Wykorzystanie technologii IP znacznie upraszcza instalację rozproszonego systemu monitoringu, który może objąć swoim zasięgiem budynki znacznie od siebie oddalone. O ile instalacja na nowo wybudowanym osiedlu nie sprawia większych problemów, o tyle modernizacja istniejącego systemu monitoringu wymaga przeprowadzania dokładnej analizy jego funkcjonowania

Firma Bestgo.pl otrzymała zlecenie zainstalowania systemu monitoringu wizyjnego na terenie osiedli mieszkaniowych dwóch spółdzielni: w Jelczu – Laskowicach oraz we Wrocławiu. W Jelczu – Laskowicach instalacja miała objąć zarówno kilkadziesiąt już istniejących budynków, jak i nowe osiedle z sześcioma budynkami, natomiast we Wrocławiu były to dwa nowe osiedla obejmujące siedem budynków.

Głównym celem wdrożenia systemów było podwyższenie poziomu bezpieczeństwa mieszkańców poprzez nadzorowanie wjazdów na teren osiedla, placów zabaw, parkingów oraz miejsc szczególnie narażonych na kradzieże czy dewastację mienia, a więc obszarów wymagających dużego zagęszczenia kamer – zarówno obrotowych, jak i stacjonarnych.

Rozwiązanie

Na terenie osiedla spółdzielni w Jelczu-Laskowicach istniał już wcześniej zbudowany system monitoringu wykorzystujący transmisję radiową. Użyte tam urządzenia narzucały ograniczenia, takie jak spore opóźnienia w transmisji i stopklatki. Ponadto jakość transmitowanego materiału była zależna od pogody. Postanowiono gruntownie zmienić infrastrukturę i, za radą Bestgo.pl, wykorzystać światłowodową transmisję sygnału wizyjnego ze wszystkich kamer bezpośrednio do centrum monitoringu. Rozwiązało to wszystkie problemy z jakością obrazu, a cały system monitoringu znacznie zyskał na funkcjonalności i sprawności.

Urządzenia umożliwiające podgląd obrazów w centrum monitorującym oraz archiwizację materiału wizyjnego zostały zainstalowane w szafach typu rack umieszczonych w profesjonalnych serwerowniach – z klimatyzacją i zasilaniem awaryjnym.

Fot. 1. Kamera ACTi KCM-5111

Fot. 2. Rejestrator QNAP VioStor VS-8040U

Korzyści

Korzyści, jakie osiągnięto dzięki uruchomieniu systemu monitorującego, mają wymiar społeczny, przede wszystkim prewencyjny. Ze zgromadzonego materiału wizyjnego bardzo często korzystają służby mundurowe czy pracownicy administracji spółdzielni. Wielokrotnie udało się zidentyfikować sprawców zdarzeń właśnie dzięki tym nagraniom.

Na obu osiedlach mieszkaniowych zastosowano kamery firmy ACTi – w sumie 92 kamery IP. Wybrano trzy modele kamer, w tym kamery szybkoobrotowe, kompaktowe kamery 4-megapikselowe oraz kamery typu *bullet* o rozdzielczości 1.3 Mpix. Kamery ACTi zostały wybrane ze względu na wysoką rozdzielczość i jakość obrazu, duży wybór modeli oraz możliwość zasilania kamer metodą PoE. Dodatkowym atutem tego rozwiązania było współdziałanie kamer ACTi z różnymi systemami rejestracji obrazu, dzięki czemu inwestor miał bardzo duży wybór dostępnych na rynku rejestratorów. Ponadto kamery ACTi są objęte trzyletnią gwarancją z możliwością przedłużenia jej do ośmiu lat. Inwestor zdecydował się na zastosowanie rejestratorów firmy QNAP z procesorem Intel Core 2 Duo 2.8 GHz ze względu na ich niezawodną pracę i dużą wydajność. Rejestratory QNAP umożliwiają rejestrację obrazu o bardzo wysokiej rozdzielczości (do 8 Mpx). W projekcie systemów monitoringu dla wymienionych osiedli zastosowano modele 24- i 40-kanałowe umieszczone w obudowie typu rack. Wybrano modele z ośmioma kieszeniami na dyski SATA hot-swap. Rejestrator QNAP VioStor umożliwia długoterminową rejestrację obrazu o bardzo wysokiej rozdzielczości. Możliwość zastosowania wybranej konfiguracji macierzy RAID (RAID 0, RAID 1, RAID 5, RAID 5+, RAID 6, JBOD, Single Disk) daje w efekcie wysoki poziom bezpieczeństwa przechowywanych danych. Ważna była także możliwość wykorzystania inteligentnej analizy obrazu.

Infrastruktura sieciowa

W systemie zastosowano nowe przełączniki Cisco z serii Catalyst, umożliwiające tworzenie sieci szkieletowej o przepustowości 10 Gb/s, oraz zasilanie kamer metodą PoE.

Przełączniki Cisco Catalyst obsługują połączenia głosowe, wizyjne i połączenia związane z transmisją danych. Do ich głównych zalet należą kompleksowe funkcje związane z komunikacją, udoskonalone zabezpieczenia, łatwa konfiguracja oraz wysoki stopień niezawodności.

Wypowiedź instalatora

Istotnym wyróżnikiem naszej firmy jest jakość usług, która przekłada się na zadowolenie naszych klientów . Aby nie zmagać się z awariami, inwestujemy w nowoczesne technologie i markowy sprzęt. Nasza kadra przechodzi gruntowne szkolenia. Techniką cyfrowej transmisji dźwięku i obrazu zajmujemy

Fot. 3. Kamera ACTi ACM-1231

się od 2007 roku. Nasza wiedza z zakresu budowy sieci i zasad budowy systemów monitoringu wizyjnego znacząco przyczyniła się do wzrostu sprzedaży tego rodzaju usług. Mamy rozwiązania przeznaczone zarówno do małych, jak i dużych instalacji, a dodatkowo zapewniamy serwis na najwyższym poziomie.

Obecnie realizujemy równolegle kilka projektów na terenie Dolnego Śląska i optymistycznie patrzymy w przyszłość tego segmentu rynku.

Paweł Ruszczyński
Bestgo.pl

Wypowiedź dystrybutora

Dzięki bogatemu asortymentowi oferowanych urządzeń służących do budowy systemów monitoringu wizyjnego klienci firmy FEN mają możliwość skomponowania odpowiednich dla nich systemów IP z wykorzystaniem rozwiązań różnych producentów.

Doskonałym przykładem jest połączenie kamer IP firmy ACTi z sieciowym rejestratorem QNAP. Dzięki dostępnemu dla wszystkich zestawowi narzędzi programistycznych SDK (*Software Development Kit*) kamery ACTi mogą być bardzo łatwo dodawane do systemów rejestracji obrazu innych producentów. Ponadto zarówno rejestratory QNAP, jak i kamery ACTi są zgodne ze standardem ONVIF. Spółdzielnie mieszkaniowe, które zdecydowały się na zainstalowanie systemów monitoringu wizyjnego z kamerami ACTi, są bardzo zadowolone z osiągniętego rezultatu. Co najważniejsze, sieciowy system monitorujący wielokrotnie sprawdził się i umożliwił wykrycie sprawców zdarzeń zagrażających bezpieczeństwu mieszkańców.

Zastosowanie kamer megapikselowych oraz kamer obrotowych PTZ sprawiło, iż do obserwacji całego obszaru osiedla zastosowano trzykrotnie mniej kamer niż potrzeba w przypadku systemów analogowych proponowanych przez konkurencję. Administracja budynków, policja i straż miejska są zadowolone z wysokiej jakości rejestrowanego obrazu, dzięki której identyfikacja sprawców wykroczeń nie sprawia im problemów.

Anna Twardowska
Monitoring IP Business Unit Manager
Konsorcjum FEN

FAAST

FIRE ALARM ASPIRATION SENSING TECHNOLOGY®

Wykrywanie pożarów w najtrudniejszych warunkach

- Detekcja dymu oparta na technologii laserowej
- Wersja konwencjonalna lub adresowalna
- Dwustopniowy pomiar przepływu powietrza metodą ultradźwiękową
- Prosta, szybka obsługa i konfiguracja

FAAST LT łączy skuteczność technologii czujek zasysających z analogową komunikacją na pętli adresowalnej. Program do projektowania oraz elastyczność konfiguracji czujki zapewnia wszechstronne wykorzystanie nawet w najtrudniejszych warunkach.

Więcej informacji na www.faast-detection.com

Dostępne w

ADI GLOBAL DISTRIBUTION

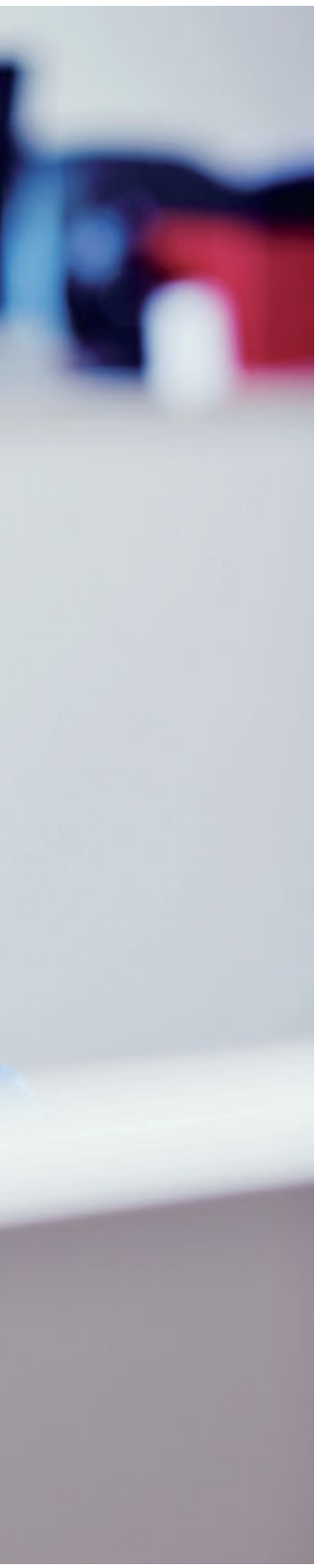
adiglobal.com/pl
info.pl@adiglobal.com

STAM-2

System wspomagania stacji monitorowania

Michał Konarski

Jedną z najważniejszych funkcji skutecznego systemu alarmowego jest sprawne powiadamianie o wykryciu zagrożenia. Gdy bezpieczeństwo jest priorytetem, niezbędna jest możliwość efektywnego odbierania, przetwarzania i właściwego reagowania na informacje przychodzące z systemów alarmowych. Te działania realizowane są przez stacje monitorowania, stanowiące centra logistyczne firm świadczących usługi ochrony. Efektywna realizacja zadań stacji monitorującej wymaga odpowiedniej infrastruktury, w tym specjalistycznego sprzętu oraz oprogramowania



Z myślą o wsparciu stacji monitorowania alarmów firma SATEL opracowała modularny system STAM-2. Obejmuje on sprzęt niezbędny do odbierania informacji z instalacji alarmowych oraz oprogramowanie umożliwiające sprawne przetwarzanie napływających danych. Dzięki modularnej budowie można go łatwo dopasować do bieżących potrzeb i rozbudować w przyszłości, w miarę powiększania się bazy obsługiwanych abonentów.

Rozwiązania sprzętowe

Bazą systemu STAM-2 są karty odbiorcze umożliwiające odbieranie danych z systemów alarmowych za pomocą różnych mediów i protokołów.

Karty telefoniczne to wieloformatowe urządzenia pozwalające na odbieranie i dekodowanie transmisji odbieranych za pośrednictwem tradycyjnej linii telefonicznej (PSTN). Do obsługiwanych formatów należą rozmaite warianty formatów impulsowych 4/2, formaty DTMF, takie jak Ademco Express i ContactID, a także format modemowy SIA.

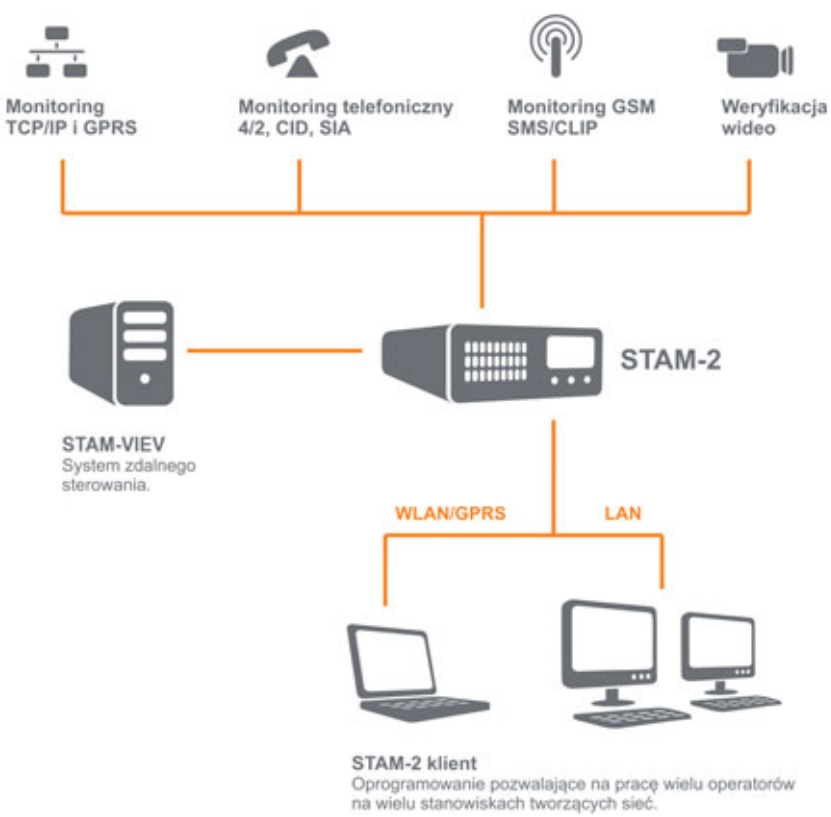
Karty ethernetowe umożliwiają zastosowanie łączności za pośrednictwem TCP/IP w monitorowaniu z wykorzystaniem urządzeń SATEL. Dzięki nim można odbierać informacje wysyłane przez moduły nadajników ETHM-1, ETHM-2 oraz nadajników firmy SATEL wykorzystujących transmisję GPRS. Dzięki zastosowaniu zaawansowanej kontroli łączności oraz szyfrowania transmitowanych danych łączność cyfrowa zapewnia dużo większą niezawodność transmisji i integralność danych niż tor telefoniczny.

Uzupełnieniem kart odbiorników telefonicznych oraz TCP/IP są moduły GSM pełniące rolę odbiorników informacji o zdarzeniach przesyłanych jako wiadomości SMS. Ten tor transmisji jest wykorzystywany najczęściej jako zapasowy w przypadku nadajników korzystających z transmisji GPRS, ewentualnie jako tor podstawowy w przypadku instalacji o niższym stopniu zabezpieczenia. Moduły GSM umożliwiają także odbieranie danych transmitowanych w technologii CSD, która może być wykorzystywana przez nadajniki GSM SATEL tam, gdzie niedostępne są usługi GPRS.

W systemie STAM-2 może funkcjonować równocześnie wiele odbiorników, w zależności od liczby obsługiwanych abonentów oraz liczby fizycznych łączy (np. linii telefonicznych). Ponadto kolejne odbiorniki mogą być instalowane w miarę rozbudowywania bazy klientów stacji w celu zapewnienia dostępności łączy na odpowiednim poziomie.

Urządzenia odbiorcze systemu STAM-2 są podłączane do centralnego serwera obsługującego bazę danych abonentów oraz zdarzeń. W zależności od wielkości i potrzeb stacji monitorującej dostępne są różne rozwiązania.

W przypadku mniejszych stacji najlepszym rozwiązaniem jest STAM-IRS. Łączy on w przemysłowej obudowie 19-calową platformę-bazę do instalacji kart odbiorników



Rys 1. Struktura systemu wspomagania stacji monitorowania STAM-2

Fot. 1. Odbiornik stacji monitorowania z wbudowanym mikroserwerem STAM-IRS

Fot. 2. Obudowa z zasilaczem do kart stacji monitorującej STAM-BOX

(do 14 odbiorników telefonicznych i Ethernet, do 3 modułów GSM), mikroserwer Intel Atom z magazynem SSD i wyświetlaczem TFT 7" oraz buforowy zasilacz do kart odbiorczych i serwera. W przypadku STAM-IRS system operacyjny oraz serwer STAM-2 są już wstępnie zainstalowane, co ogranicza do niezbędnego minimum kwalifikacje potrzebne do uruchomienia stacji.

Jeżeli potrzeby stacji przekraczają możliwości oferowane przez energooszczędny serwer z procesorem Intel Atom, rozwiązaniem może być zastosowanie platformy STAM-BOX. Zawiera ona płytę bazową umożliwiającą instalację kart odbiorczych oraz wbudowany zasilacz buforowy zapewniający nieprzerwane zasilanie odbiorników. Podobnie jak STAM-IRS, STAM-BOX ma 19-calową obudowę ułatwiającą montaż w szafach ze sprzętem infrastrukturalnym. W celu gromadzenia i przesyłania danych odbiorniki umieszczone w platformie STAM-BOX muszą zostać przyłączone do zewnętrznego serwera, którego parametry będą dopasowane do potrzeb zależnych od liczby abonentów oraz stanowisk dyspozytorskich (stacji roboczych) korzystających z zasobów serwera.

Oprogramowanie

System STAM-2 wykorzystuje architekturę klient-serwer. Dane transmitowane różnymi torami trafiają do centralnej bazy danych zarządzanej przez aplikację STAM-SERVER na serwerze systemu STAM-2. Z tym serwerem łączą się stacje robocze dyspozytorów, oferując wizualizację napływających danych oraz wspierając logistykę obsługi zdarzeń. Stacje robocze łączą się z serwerem przez sieć lokalną, można też wykorzystać w tym celu technologię tunelowania i zdalnego dostępu do zasobów serwera.

Oprócz typowych informacji o zdarzeniach serwer STAM-2 potrafi również odbierać i gromadzić sekwencje obrazów z systemów wizualnej weryfikacji alarmów VIVER, które mogą stanowić doskonałe uzupełnienie ogólnej informacji o wykrytym zagrożeniu. W przeciwieństwie do standardowej funkcji zdalnego dostępu do rejestratorów obrazu nie ma konieczności ręcznego wyszukiwania najważniejszej sekwencji w pamięci urządzenia. W przypadku transmisji z modułów VIVER sekwencja obrazów powiązana z danym zdarzeniem alarmowym zostanie automatycznie przypisana do tego zdarzenia na poziomie bazy danych. Dzięki temu operator stacji może zapoznać się z materiałem wizyjnym weryfikującym zdarzenie bezpośrednio podczas obsługi tego zdarzenia.

Podstawowym środowiskiem pracy dyspozytorów jest aplikacja STAM-KLIENT pracująca w systemie Windows. Umożliwia ona łatwy i szybki dostęp do napływających na bieżąco informacji o zdarzeniach, udostępniając narzędzia ułatwiające podejmowanie odpowiednich czynności w zależności od rodzaju zdarzenia. Ponadto konieczność podjęcia właściwych działań jest sygnalizowana przez pojawiające się okna.

Oprócz bieżącej obsługi aplikacja kliencka umożliwia sprawne filtrowanie zdarzeń, tworzenie raportów i zestawień oraz prezentację danych w postaci tablic synoptycznych i wizualnych map monitorowanych obiektów.

Dużym udogodnieniem dla dyspozytorów, wprowadzonym w systemie STAM-2, jest mechanizm wewnętrznej komunikacji poprzez notatki. Notatki takie mogą być adresowane do konkretnych użytkowników systemu lub rozgłaszane. Można również określić czas ich ważności.

Ciekawym rozszerzeniem systemu STAM-2 jest system zdalnego dostępu STAM-VIEW. Jego zadaniem jest udostępnienie bieżących informacji o wybranych zdarzeniach użytkownikom spoza stacji – instalatorom, administratorom systemów alarmowych, a nawet użytkownikom końcowym. STAM-VIEW udostępnia tym użytkownikom wiele narzędzi ułatwiających dostęp – mechanizmy wyszukiwania, filtrowania zdarzeń czy komunikacji wewnętrznej. Dzięki temu dyspozytorzy stacji monitorującej nie muszą udzielać

Fot. 3. Wizualna weryfikacja alarmu z użyciem modułu VIVER

Fot. 4. System zdalnego podglądu zdarzeń STAM-VIEW

informacji o zdarzeniach przez telefon, więc mogą w większym stopniu skoncentrować się na swoich podstawowych obowiązkach.

Ze względu na bezpieczeństwo dostępu do informacji zawartych w bazie danych, system STAM-VIEW powinien być instalowany na dodatkowym serwerze, niezależnym od głównego serwera STAM-2. W celu ułatwienia instalacji i konfiguracji STAM-VIEW jest dystrybuowany w postaci łatwej w użyciu wirtualnej maszyny.

Warto również wspomnieć o systemie STAM-2 PRO, który ma podstawowe funkcje stacji monitorującej i umożliwia zdalne zarządzanie systemami alarmowymi INTEGRA wyposażonymi w moduły ETHM-1. Można go wykorzystać na przykład w ochronie placówek bankowych rozmieszczonych na terenie całego kraju.

Firma SATEL oferuje szkolenia w zakresie instalowania, uruchamiania i zarządzania systemami STAM-2. Na szkoleniach można zdobyć wiedzę niezbędną do umiejętnego wykorzystywania możliwości systemu i zapewnienia jego prawidłowego działania.

Michał Konarski
SATEL

Niewidzialna ochrona domu

ATLine

Masz piękny dom, na który pracowałeś latami? Chcesz, żeby był bezpieczny, ale nie chcesz szpecić posesji kamerami i wysokimi ogrodzeniami? Można sprawić, by posiadłość budziła zachwyt i jednocześnie była chroniona przed intruzami. Rozwiązaniem jest zastosowanie niewidocznego, ukrytego pod ziemią systemu ostrzegania

Piękne domy od zawsze przyciągają uwagę złodziei. Już w czasach zamierzchłych budowano olbrzymie mury i kopano głębokie fosy, które miały chronić przed intruzami. Mimo iż dziś technika umożliwia użycie subtelniejszych środków, wciąż podstawową formą ochrony są wysokie płoty, mury czy ogrodzenia.

Samo ogradzanie jednak nie wystarczy. Chcemy wiedzieć o obecności niepożądanych gości, dlatego bardzo popularne są kamery na prywatnych posesjach, ale nadzór z użyciem kamer i wysokie mury sprawiają, że przytulny, stylowy dom zaczyna przypominać więzienie, a jego mieszkańcy mogą czuć się jak bohaterowie filmu *Skazani na Shawshank*. Różnica polega na tym, że przebywają w nim dobrowolnie. Piękny dom i ogród mają cieszyć oko, chcemy się nimi chwalić, a wysokie ogrodzenia eliminują taki efekt. Spacer po ogrodzie obwieszonym kamerami może skojarzyć się z przechadzką po spacerniaku.

Na szczęście współczesna technika jest coraz doskonalsza, a rozwiązania, które mają chronić nas przed obcymi, są coraz bardziej wyrafinowane – od dobrze znanych, takich jak zdalnie sterowana pilotem brama, dzięki której możemy wjechać na posesję bez wysiadania z auta, po bardziej zaawansowane, takie jak np. kamery termowizyjne. W najnowocześniejszych rezydencjach używa się dziś zakopywanych w ziemi obwodowych systemów ostrzegania.

W Polsce takie rozwiązania już się pojawiły. Absolutną nowością są zdobywające wielu zwolenników zakopywane systemy połączonych sensorów. Jak działa taki system? Z wyglądu przypomina kabel z umieszczonymi co kilkadziesiąt centymetrów

czujnikami. Jego działanie opiera się na wyczuwaniu zmian nacisku na podłoże, a jego podstawową zaletą jest niewidzialna i niewykrywalna strefa detekcji, którą możemy wyznaczyć zgodnie z naszymi potrzebami.

– Na głębokości około 60 centymetrów pod ziemią, co około 90 centymetrów umieszczane są specjalne czujniki wykrywające fale sejsmiczne generowane przez osobę idącą po powierzchni gruntu. Nieważne, czy powierzchnię tę tworzy trawa, żwir, asfalt czy kostka brukowa. – wyjaśnia Sławomir Pruski, właściciel firmy ATLine, która ma w swojej ofercie system DEA Sisma CP.

Co istotne, konstrukcja, zastosowane czujniki oraz zaawansowane funkcje analityczne układów przetwarzania gwarantują dużą odporność na zmienne warunki klimatyczne. Nieważne, czy jest bardzo zimno, czy panuje 35-stopniowy upał – ten system działa niezawodnie. Tym, co wyróżnia omawiane rozwiązanie i odróżnia je od innych obecnych na rynku, jest brak potrzeby konserwowania części zakopywanych. Raz zakopany system nie musi być wydobywany z ziemi dzięki temu, że jest to system modułów, które można niemal dowolnie łączyć i dzielić, a nie pojedynczy kabel. Strefę wykrywania intruzów można wyznaczyć dowolnie, dopasowując ją do ukształtowania terenu. Można ominąć przeszkody, takie jak drzewa czy kępy krzewów. Zakopywane podzespoły nie zawierają żadnych aktywnych części elektronicznych, dzięki czemu są niewrażliwe na wszelkie awarie i uszkodzenia natury elektrycznej.

W momencie, gdy ktoś niepożądany wejdzie na pas detekcji, który ma około półtora metra szerokości, właściciel posesji zostanie o tym powiadomiony. Kalibrację i programowanie systemu można przeprowadzić na domowym komputerze. Proste w obsłudze oprogramowanie wyświetla w czasie rzeczywistym przebiegi sygnałów nadchodzących z każdego czujnika. Moduł przetwarzania jest wyposażony w pamięć o dużej pojemności, a wszystkie sygnały nadchodzące z czujników są zapisywane chronologicznie. Pamięć ta umożliwia użytkownikom systemu przeprowadzenie dokładnej analizy zarejestrowanych zdarzeń i ewentualnie określenie przyczyny wywołania alarmu. System detekcji potrafi też rozróżnić różne typy wtargnięć i odfiltrowuje zakłócenia jako źródła fałszywych alarmów (np. zakłócenia wywołane przez niekorzystne warunki atmosferyczne).

Alarm może być sygnalizowany za pomocą powszechnie stosowanych sygnalizatorów świetlnych czy dźwiękowych,

Fot. 1. System składa się z czujników połączonych kablem, które reagują na zmiany nacisku w obrębie niewidzialnej strefy detekcji

Fot. 2. Czujniki zakopane na głębokości ok. 60 cm pod ziemią wykrywają fale sejsmiczne generowane przez intruza na powierzchni – niezależnie od rodzaju wierzchniego podłoża, po którym się porusza

a informacja o alarmie przekazywana telefonicznie, za pośrednictwem SMS lub, w zależności od wyposażenia obiektu, bezpośrednio do programu zarządzającego lub przez e-mail. Dzięki połączeniu systemu z urządzeniami mobilnymi właściciel posesji może zostać powiadomiony o intruzie, będąc daleko od domu – na wczasach czy na wyjeździe służbowym. Wszystko zależy od rytmu życia domowników – opcja powiadomienia powinna być dostosowana do ich potrzeb.

Gdzie montowany jest system? – *Zakopywane systemy ostrzegania najczęściej montujemy na podjazdach przed garażami. To dodatkowo chroni stojące w nich samochody. Często także pod oknami na parterze. W przeciwieństwie do krat system nie szpeci okien, a spełnia podobną funkcję. Może znajdować się też w dowolnym miejscu ogrodu. Najlepiej zakopać go wzdłuż ogrodzenia – intruz może dostać się na teren posesji, ale zostanie natychmiast wykryty i zlokalizowany.* – mówi Sławomir Pruski.

Jedyną wadą niewidzialnej z zewnątrz ochrony jest brak odstraszania potencjalnego złodzieja, dlatego warto umieścić na płocie, bramie lub furtce informację o tym, że dom jest pod ochroną.

ATLine

Fot. 3. Konstrukcja modułów umożliwia niemal dowolne wyznaczenie strefy detekcji, niezależnie od ukształtowania terenu, dzięki czemu system jest uniwersalnym rozwiązaniem dla każdej posesji

Nowoczesny budynek bez kluczy

Marek Adameczek
Agnieszka Filipowicz

Kontrola dostępu to niezbędny podsystem kompleksowego systemu zarządzania budynkiem. Ze względu na bardzo wysokie i ciągle rosnące wymogi bezpieczeństwa obiektów sprawne zarządzanie kontrolą dostępu w całym budynku jest w dzisiejszych czasach jednym z najważniejszych zadań systemów zabezpieczeń. Jednocześnie istotnym problemem stało się zarządzanie kluczami mechanicznymi w nowoczesnych budynkach

Fot. 1. Okucie do drzwi szklanych

Nawet najlepszy system, w którym wykorzystywane są klucze mechaniczne, ma wiele poważnych wad – jest bardzo uciążliwy, a zarządzanie nim jest kosztowne. Klucz można łatwo skopiować lub zgubić, a efektem jest konieczność wymiany wkładki i zastosowania nowego klucza. Zamknięcia na klucz mechaniczny nie spełniają współczesnych wymogów i standardów bezpieczeństwa. W Europie Zachodniej już od kilku lat promowana jest idea budynków bez klucza mechanicznego. Do zarządzania dostępem do wszystkich pomieszczeń w budynku służą elektroniczne okucia i wkładki. Klucz mechaniczny został całkowicie zastąpiony kluczem elektronicznym w postaci karty zbliżeniowej, breloka itp.

Chociaż koncepcja zamka sterowanego kartą zbliżeniową nie jest nowa, najnowsza technologia SALTO Virtual Network (SVN) jest rozwiązaniem nowatorskim, o niespotykanych możliwościach. Jej zastosowanie, oprócz zamiany klucza mechanicznego na elektroniczny, wprowadza kontrolę dostępu w świat technologii bezprzewodowych. Przynosi to dodatkowe korzyści w postaci obniżenia kosztu i czasu instalacji.

W systemie kontroli dostępu firmy SALTO Systems nie ma okablowania, dlatego każda zmiana w budynku, skutkująca nową konfiguracją drzwi, jest bardzo prosta do przeprowadzenia. Możemy na przykład z łatwością zamontować drzwi, których skrzydło wykonane jest z tafli szkła zamiast drewna, a także podzielić większe pomieszczenia na mniejsze, zwiększając liczbę kontrolowanych przejść. Dostosowanie okablowanego systemu do nowych wymagań bywa kosztowne i czasochłonne. Niekiedy zmiana sposobu wykorzystywania obiektu i konieczność objęcia kontrolą dostępu nowych pomieszczeń spotyka się z oporem konserwatora zabytków. Unikniemy tego typu problemów, stosując nowoczesny system bezprzewodowy.

Jak działa technologia SVN?

Zamki pracują w sieci wirtualnej (SVN) i są połączone z systemem, jednak bez zastosowania kabli. Komunikację między wszystkimi urządzeniami a serwerem centralnym zapewnia inteligentny klucz, który gwarantuje wszystkim użytkownikom dostęp do pomieszczeń w budynku i zarazem stanowi dwukierunkowy nośnik danych. Klucz ten może mieć postać karty zbliżeniowej, breloka lub opaski na rękę. Oczywiście jeden z czytników musi być podłączony do budynkowej sieci LAN, aby można było aktualizować dane na kartach użytkowników za pomocą pulpitu administratora. Taki czytnik on-line instaluje się w miejscu, w którym musi bywać każdy z użytkowników. Może to być na przykład kołowrót obok recepcji. Użytkownicy, wykonując swoje codzienne czynności, otwierają pomieszczenia za pomocą kart i dystrybuują niezbędne dane dotyczące uprawnień. Monitorowanie listy zdarzeń, zmiany praw dostępu, a nawet realizacja funkcji diagnostycznych systemu są wykonywane bez potrzeby fizycznego zbierania informacji z czytników i bezprzewodowych zamków.

W prawidłowo zaprojektowanym systemie SVN praktycznie nie istnieje ryzyko nieuprawnionego otwarcia drzwi. Lista kart, które straciły ważność, jest aktualizowana przez czytnik podłączony do budynkowej sieci LAN i zapisywana przez niego na wszystkich kartach w systemie, które miały z nim styczność. Co więcej, informacja o utraconych uprawnieniach jest zapisywana także w zamkach, które miały styczność z kartą, na której czytnik podłączony do budynkowej sieci LAN zapisał aktualną wersję czarnej listy.

Fot. 2. Wkładki elektroniczne GEO

Fot. 3. Okucie z klawiaturą

System łączności bezprzewodowej

Czasami zachodzi potrzeba zdalnego sterowania wszystkimi lub niektórymi drzwiami w budynku w czasie rzeczywistym, na przykład awaryjnego otwarcia lub zablokowania drzwi w sytuacji zagrożenia zamachem terrorystycznym. Wtedy konieczna jest natychmiastowa łączność z zamkiem, jaką daje kabel lub połączenie radiowe (bezprzewodowe). System SALTO można uzupełnić o bramki bezprzewodowe. Umieszcza się je w punktach o dobrej „widoczności radiowej", podobnie jak punkty dostępowe Wi-Fi. Każda z bramek nawiązuje łączność w czasie rzeczywistym z zamkami w zasięgu kilkudziesięciu metrów. Jedna bramka może połączyć się z nawet kilkunastoma zamkami wyposażonymi w moduł radiowy. Dzięki takiemu rozwiązaniu operator uzyskuje całkowitą kontrolę nad drzwiami – m.in. sygnalizowany jest stan drzwi i naciśnięcie klamki wewnętrznej.

Fot. 4. Biocote – ochrona antybakteryjna

Zamek do każdych drzwi

Systemy SALTO można zastosować w praktycznie każdym miejscu wymagającym kontroli dostępu. Zarówno same zamki, jak i funkcje oprogramowania można dobrać tak, aby jak najlepiej odpowiadały oczekiwaniom użytkowników.

Zamki mogą mieć postać okuć – podobnych do tych, jakie możemy spotkać w hotelach (ale bardziej wytrzymałych) – lub elektronicznych wkładek DIN z czytnikiem kart i układem sterującym. Dostępne są także okucia do drzwi szklanych oraz wzmocnione kłódki wykorzystywane w transporcie i magazynach.

Z myślą o szatniach i szafkach na leki opracowano zamek wyposażony w specjalne funkcje.

Mając na uwadze wymóg zwiększonej wytrzymałości mechanicznej, opracowano zamki wzmocnione, które sprawdzą się w budowlach infrastrukturalnych, takich jak elektrownie czy zapory wodne. Otrzymały one holenderski certyfikat odporności przeciwwłamaniowej SKG.

Specjalna powłoka Biocote jest przeznaczona do zastosowania w szkołach, szpitalach, restauracjach oraz laboratoriach, gdzie istnieje poważne ryzyko zakażenia bakteriologicznego. Powłoka antybakteryjna zapobiega rozprzestrzenianiu się drobnoustrojów.

Nowoczesne rozwiązania dla sektora edukacyjnego obejmują integrację uczelnianej i kampusowej kontroli dostępu z elektroniczną legitymacją studencką.

Urządzenia bezprzewodowe, takie jak wirtualna sieć SVN, z powodzeniem zastępują tradycyjną instalację kablową w kontroli dostępu. Mają takie same funkcje w zakresie kontroli nad przejściem jak systemy kablowe, ale są zdecydowanie prostsze i tańsze w instalacji. Łatwość, z jaką wprowadza się zmiany do systemu, jest szczególnie widoczna przy przebudowie pomieszczeń. Oszczędność czasu, pracy i materiałów ma wyraźny aspekt finansowy.

SALTO Systems to młoda, prężna firma o dużych osiągnięciach. W okresie dwunastu lat jej istnienia na całym świecie zainstalowano ponad 1,2 miliona wyprodukowanych przez nią zamków. Największe instalacje mogą obsługiwać do 64000 użytkowników. Szacuje się, że technologią firmy SALTO posługuje się na co dzień na świecie ponad 10 milionów użytkowników. Wyrazem zaangażowania się firmy SALTO w działania na polskim rynku jest nowo otwarte biuro przedstawicielskie w Warszawie. Zainteresowani funkcjonowaniem Salto Virtual Network oraz rozwiązaniami stworzonymi na potrzeby bezprzewodowej kontroli dostępu znajdą tam profesjonalną pomoc.

Marek Adameczek
Agnieszka Filipowicz

Salto Systems
Oddział w Polsce
ul. Ostrobramska 101a, 04-041 Warszawa
e-mail: kontakt@saltosystems.com
www.saltosystems.pl

SAMSUNG

Kompaktowe · Stylowe · HD · W przystępnej cenie

LiteNet

Odwiedź: litenet.samsungsecurity.co.uk

Kamery o rozdzielczości 1,3 i 3 megapikseli zapewniają bardzo dobry obraz w przystępnej cenie. Zastosowane technologie: Transmisja wielostrumieniowa, funkcje Smart Codec i Progressive Scan — wszystkie przyczyniają się do rejestrowania wyraźniejszych, ostrych obrazów.

Kamery sieciowe LiteNet firmy Samsung są przeznaczone do instalacji w systemach o dowolnej wielkości.

Niedrogie rozwiązania megapikselowe już dostępne w sieci blisko Ciebie!

E STEsecurity@samsung.com
W samsungsecurity.co.uk

Samsung Techwin Europe Ltd

Abloy Protec Cliq

Zdalnie programowany system zamknięć od Assa Abloy

Grzegorz Korzeniowski

Assa Abloy, globalny lider produkcji kompleksowych systemów zabezpieczeń budynków, wprowadza wiele rewolucyjnych rozwiązań podwyższających standardy zabezpieczeń obiektów. Jednym z nich jest Abloy Protec Cliq. Innowacyjny system zamknięć integrujący rozwiązania mechaniczne i elektroniczne znajduje szereg zastosowań w obiektach wymagających specjalnych zabezpieczeń

Technologia Cliq + mechaniczny system Abloy Protec

Innowacyjność nowoczesnego rozwiązania Assa Abloy wynika z połączenia technologii Cliq i mechanicznego systemu Abloy Protec. Technologia Cliq umożliwia instalację zaawansowanej elektroniki w kluczach i wkładkach. Dzięki niej administrator systemu ma m.in. możliwość zdalnego nadawania lub odbierania uprawnień poszczególnym użytkownikom czy śledzenia dzienników zdarzeń. Z kolei Abloy Protec to spełniające najbardziej rygorystyczne wymogi tradycyjne mechaniczne elementy wchodzące w skład systemu zabezpieczeń budynku – klucze, wkładki, kłódki. To rewolucyjne połączenie jest gwarantem elastyczności, funkcjonalności i bezpieczeństwa. Inteligentny, zdalnie programowany system sprawdzi się wszędzie tam, gdzie konieczna jest niezawodność i najwyższy poziom zabezpieczenia.

Abloy Protec Cliq może być częścią idealnie dopasowanego do potrzeb danego przedsiębiorstwa systemu klucza generalnego Dzięki takiemu systemowi każdy użytkownik posługuje się tylko jednym kluczem, dzięki któremu może dostać się do wielu pomieszczeń (ich liczba może być nieograniczona), przy czym do otwarcia drzwi potrzebne jest uprawnienie.

Elastyczność i bezpieczeństwo

W skład systemu Abloy Protec Cliq wchodzą klucze użytkowników i klucze programujące (w tym główny klucz programujący), które są identyfikatorem systemu wobec programatora i oprogramowania. Dzięki nim mamy możliwość zaprogramowania wkładek oraz odczytu pamięci zdarzeń. Do systemu należą także wkładki/cylindry i kłódki oraz wspomniany wyżej programator i oprogramowanie zawierające bazę danych systemu.

Mnogość elementów nie oznacza skomplikowanego zarządzania systemem. Jego administrator może programować system w prosty sposób, np. tworząc grupy użytkowników o różnych uprawnieniach mechanicznych i elektronicznych, a także tworząc strefy, do których dostęp mają jedynie pojedyncze osoby. Abloy Protec Cliq pozwala również na stworzenie tzw. czarnej listy, za pomocą której koryguje się ustawienia grupowe dla pojedynczych użytkowników. Istnieje prosty sposób nadania, odebrania lub zmiany praw użytkowników systemu. Z perspektywy zarządcy obiektu czy właściciela firmy bardzo istotna jest także możliwość kontroli. We wchodzące w skład systemu klucze i cylindry wbudowane są dzienniki zdarzeń. Użycie każdego klucza użytkownika powoduje zapis daty, godziny i ID wkładki w pamięci klucza. W zależności od rodzaju zapamiętuje on od 100 do 1800 ostatnich zdarzeń. Dzięki temu istnieje możliwość śledzenia, w jakim czasie i przez którego użytkownika klucz był używany do otwierania poszczególnych zamków. Możemy zweryfikować również informacje dotyczące konkretnego cylindra. Wkładka „zapamiętuje" maksymalnie 1000 ostatnich zdarzeń, w tym 20 ostatnich prób dostępu z wykorzystaniem nieautoryzowanych kluczy.

W systemie Abloy Protec Cliq baterie zasilające umieszczone są jedynie w kluczach; nie ma potrzeby zasilania wkładek, więc nie jest potrzebne okablowanie. Ponadto bateria w kluczu umożliwia zaprogramowanie funkcji czasowej. Elektroniczne klucze mogą być ustawione jako aktywne na pewien czas, uzależniony np. od harmonogramu pracy danego pracownika.

Rozwiązanie firmy Assa Abloy gwarantuje wysoki i niezmienny poziom bezpieczeństwa. W razie zaginięcia klucza nie musimy wymieniać wkładki czy przeprogramowywać systemu. W prosty i szybki sposób możemy zmienić uprawnienia

Fot. 1. Abloy Protec Cliq

nadane zgubionemu elementowi. Co więcej, uprawnienia do dostępu mogą być nadawane i odbierane zdalnie. Właściciel firmy czy zarządca obiektu kieruje całym systemem za pomocą laptopa. Może na przykład wydać klucze poszczególnym pracownikom pracującym w terenie i uaktywnić je w ustalonym czasie – zdalnie, w swoim biurze. Daje to możliwość zarządzania dużym obszarem, w tym jednoczesnej kontroli kilku budynków znacznie oddalonych od siebie.

Szereg korzyści

Abloy Protec Cliq oferuje szereg korzyści widocznych z perspektywy zarządzania, funkcjonowania obiektu czy jego administracji.

Wybór Abloy Protec Cliq to rozwiązanie tańsze niż zakup różnych urządzeń, które razem zabezpieczałyby obiekt w podobny sposób. Koszty instalacji i utrzymania systemu są niskie i można go długo użytkować.

Klucz Abloy Protec Cliq jest równie łatwy w użyciu jak standardowy mechaniczny klucz. Montaż systemu jest łatwy, ponieważ wkładka elektroniczna może zostać zamontowana w drzwiach bez zmiany już istniejących okuć i zamków. Baterie zasilające znajdują się w kluczach, więc nie jest potrzebne okablowanie.

Połączenie rozwiązań mechanicznych i elektronicznych to podwójne zabezpieczenie. Wpływ na bezpieczeństwo ma także pełna kontrola kluczy oraz możliwość szybkiej i prostej zmiany uprawnień nadanych zagubionym elementom.

Abloy Protec Cliq umożliwia łatwą rozbudowę, programowanie, dodawanie lub usuwanie kluczy, a także zmianę kombinacji kodów cylindra. Cylindry Abloy Protec Cliq mogą być dopasowane do zastosowanych mechanicznych systemów zamknięć.

Obecnie zarządzający obiektami miewają problem z pogodzeniem potrzeby pozostawienia budynku otwartym z koniecznością jego zabezpieczenia. Obiekty użyteczności publicznej, takie jak szpitale czy uniwersytety, z jednej strony powinny być dostępne i otwarte do późnych godzin nocnych, z drugiej zaś muszą być należycie chronione. Abloy Protec Cliq umożliwia dopasowanie systemu do konkretnego budynku. Administrator obiektu użyteczności publicznej ma możliwość wydzielenia specjalnych stref o różnych poziomach dostępu, zapewnienia należytego bezpieczeństwa sprzętu i pracowników, a także pełnej kontroli personelu.

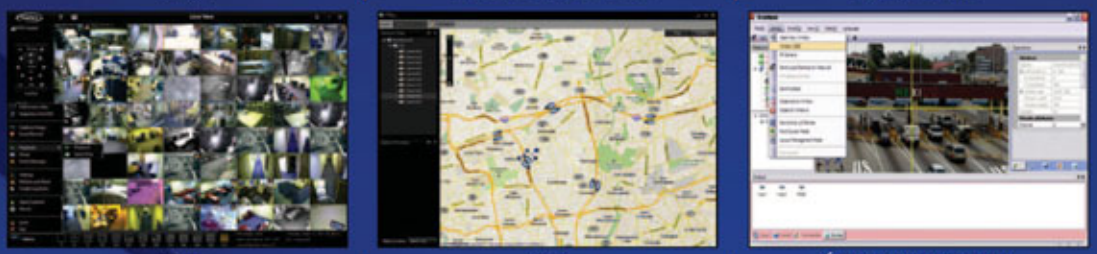
Rozwiązanie firmy Assa Abloy doskonale sprawdzi się także w miejscach, w których poziom bezpieczeństwa musi być nieprzerwanie najwyższy – może je wykorzystać na przykład branża wodociągowa, energetyczna czy wojsko. W ich przypadku luki w systemie mogą skutkować ogromnymi zniszczeniami, stratami finansowymi, a nawet zagrożeniem dotyczącym dużych grup osób. Abloy Protec Cliq jest stworzony z myślą o budynkach, w których system zabezpieczeń musi być niezawodny. Ze względu na trwałość i odporność jego elementów zastosowanie go jest najlepszym rozwiązaniem również w przypadku trudnych warunków środowiskowych.

Grzegorz Korzeniowski
Assa Abloy

OCHRONA OBWODOWA OBIEKTÓW CCTV

ZBAR

CMS + ANALIZA OBRAZU + ŚLEDZENIE



DVR + GIS + ŚCIANA WIZYJNA

POWIADOMIENIA + NVR + KONTROLA DOSTĘPU

_ 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"

_ "Command centre in-a-box"

- pierwszy na świecie system przedstawiający sytuację panującą na obiekcie za pomocą jednego serwera
- inteligentna analiza obrazu
- DVR - kamery analogowe
- NVR - kamery IP
- wspólna platforma operacyjna, która wyświetla informacje przy użyciu technologii Video Wall (do 40 monitorów)
- wspiera otwarte standardy producentów kamer
- posiada m.in. złącza: DVI, HD RGB, VGA, SDI, Ethernet
- możliwość równoległej obsługi przez kilku operatorów

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

Grundig CCTV
wyłącznie w ofercie C&C Partners Telecom

Konrad Staniewski

Z dniem 1 stycznia 2013 r. firma C&C Partners Telecom, jeden z największych w Polsce dostawców kompleksowych rozwiązań w dziedzinie telekomunikacji, teleinformatyki i zabezpieczeń, rozszerzyła swoją ofertę o produkty Grundig CCTV. Stała się również wyłącznym dystrybutorem produktów Grundig CCTV w Polsce

GRUNT TO GRUNDIG

Historia firmy Grundig, niemieckiego potentata w dziedzinie elektroniki użytkowej, sięga wczesnych lat powojennych, kiedy to Max Grundig, sprzedawca urządzeń radiowych, dostrzegając potrzebę rynku, rozpoczął seryjną produkcję odbiorników Heinzelmann, które w krótkim czasie stały się „bestsellerem" na skalę światową. Nastąpił dynamiczny rozwój firmy, szybko przyszły kolejne sukcesy. Grundig stał się największym wytwórcą odbiorników radiowych w Europie. Już w 1951 r. powstała nowa fabryka, w której wyprodukowano pierwszy telewizor.

Zgodnie z własną strategią Grundig miał stać się wielosystemowym dostawcą urządzeń w sektorze wizyjnym. W 1984 r. firma rozpoczęła produkcję magnetowidów i innych urządzeń pracujących w systemie VHS, który z czasem stał się wiodącym rozwiązaniem na rynku.

Obecnie Grundig posiada w swojej ofercie także rozwiązania CCTV, obejmujące szeroką gamę konkretnych produktów. Tworzy rozwiązania dla technologii IP, HD-SDI oraz telewizji analogowej.

Te zaawansowane systemy CCTV tworzone przez firmę Grundig łączą w sobie doskonały poziom techniczny i nowoczesność z wysokim standardem wykonania, wyjątkową funkcjonalnością i niezawodnością. Wykorzystują najnowsze technologie, a ponadto zostały opracowane z myślą o łatwej obsłudze.

Kamery kompaktowe, kopułkowe, tubowe i szybkoobrotowe mogą służyć zarówno do nadzorowania wnętrz, jak i do obserwacji obszarów leżących na zewnątrz chronionych obiektów. Obraz przekazywany przez te kamery odznacza się najwyższą jakością. Rejestracja obrazów w czasie rzeczywistym z możliwością ich podglądu na żywo uzupełnia zestaw podstawowych funkcji, jakich wymaga się od technologii CCTV.

Fot. 1. Rejestrator sieciowy NVR, model GRI-K1104A

Fot. 2. Kamera HD-SDI kopułkowa wandaloodporna z promiennikiem, model GCH-K0326V

Technologia IP

Rozwiązania CCTV IP firmy Grundig obejmują bogatą ofertę kamer kompaktowych, kopułkowych i szybkoobrotowych przeznaczonych zarówno do zastosowań wewnętrznych, jak i zewnętrznych. Uzupełnieniem oferty są odpowiednie modele rejestratorów pozwalających na automatyczną konfigurację systemu. Produkty te spełniają wszystkie wymogi wynikające z norm dotyczących telewizji dozorowej.

Kamery firmy Grundig oferują wysoką jakość obrazu bez względu na szybkość ruchu obserwowanych obiektów. Możliwy jest wybór rozdzielczości 720p HD lub 1080p Full HD z rejestracją 25 kl./s w formacie 16:9. Dzięki zgodności ze standardem ONVIF kamery Grundig zapewniają współpracę z większością systemów służących do zarządzania obrazem (VMS – Video Management System).

Rejestratory Grundig IP – nowe standardy technologii nadzoru wizyjnego

Rejestratory sieciowe Grundig w odpowiednich wersjach obsługują 4, 8 i 16 kanałów, umożliwiając zapis w jakości Full HD, 1080p, 25 kl./s na każdym kanale zarówno w trybie zapisu, jak i odtwarzania.

Dzięki wbudowanemu zaawansowanemu przełącznikowi sieciowemu z funkcją PoE możliwa jest nie tylko bezpośrednia komunikacja i zasilanie sieciowych kamer Grundig, ale przede wszystkim ich automatyczna konfiguracja. Niezawodny system operacyjny Linux zapewnia bezpieczny zapis danych. Dzięki intuicyjnemu interfejsowi graficznemu proces instalacji oraz konfiguracji całego sieciowego systemu dozorowego jest tak prosty jak w systemach analogowych.

Fot. 3. Kamera HD-SDI szybkoobrotowa zewnętrzna, model GCH-K0274P

Fot. 4. Kamera analogowa serii GCA-B1xxxB

Technologia HD-SDI

Grundig ma w swojej ofercie pełny zakres urządzeń pracujących w standardzie HD-SDI. Technologia HD-SDI umożliwia transmisję nieskompresowanego sygnału wizyjnego poprzez kabel koncentryczny w czasie rzeczywistym, dzięki czemu zachowana jest wysoka jakość obrazu, znacznie lepsza od uzyskiwanej w technologii analogowej. Istotne jest również, że wykorzystuje się do tego nieskomplikowaną instalację kablową.

Kamery pracujące w systemie HD-SDI są łączone bezpośrednio z rejestratorem DVR. Takie rozwiązanie umożliwia transmisję nieskompresowanego sygnału wizyjnego o rozdzielczości 2 Mpx w czasie rzeczywistym (25–30 kl./s), bez jakichkolwiek opóźnień. Obrazy ze wszystkich kamer pracujących w systemie mogą być równocześnie rejestrowane z rozdzielczością Full HD.

Grundig jest aktywnie działającym partnerem HD CCTV Alliance, wiele wnoszącym w rozwój technologii HD-SDI. Prace dotyczą zwiększania odległości transmisji oraz rozdzielczości obrazu, a także możliwości przesyłu danych i zasilania kamer poprzez kabel koncentryczny.

Kamery szybkoobrotowe PTZ w technologii HD-SDI

Doskonałym rozwiązaniem uzupełniającym gamę produktów HD-SDI jest kamera szybkoobrotowa, pozwalająca na rejestrację obrazu w jakości Full HD 25–30 kl./s. 18-krotny zoom optyczny oraz dodatkowe funkcje – takie jak: WDR, funkcja dzień/noc z mechanicznym filtrem IR oraz kompensacją przeciwoświetlenia – pozwalają na rejestrację obrazu w różnych warunkach oświetleniowych z zachowaniem doskonałej jakości.

Bogata oferta akcesoriów montażowych i transmisyjnych ułatwia proces instalacji oraz konfiguracji całego systemu nadzoru wizyjnego.

Fot. 5. Rejestrator DVR – 32-kanałowy model GDV-B8832A

Technologia analogowa

Kamery analogowe firmy Grundig zostały zaprojektowane i wyprodukowane zgodnie z obowiązującymi normami, z zachowaniem wysokich standardów jakościowych. Dobór odpowiednich komponentów, takich jak przetworniki, procesory sygnału DSP i obiektywy, zapewnia doskonałą jakość obrazu.

Zastosowane funkcje, do których należą: WDR – rozszerzony zakres dynamiki, DNR – cyfrowa redukcja szumów oraz inteligentna analiza obrazu, sprawiają, że rozwiązania firmy Grundig idealnie spełniają stawiane im wymagania. Wszystkie kamery analogowe wykorzystują najlepsze przetworniki obrazu oraz procesory sygnałowe DSP.

Dzięki rozdzielczości poziomej 700 TVL kamery Grundig pracują wyjątkowo dobrze przy niskim poziomie oświetlenia – przekazują wyrazisty obraz. Aby sprostać wysokim oczekiwaniom użytkowników, analogowa seria kamer wyróżnia się wieloma unikatowymi funkcjami.

Rejestratory DVR pozwalają na obsługę zarówno podstawowych systemów 8-kanałowych, jak i jednostek rejestrujących 32 kanały. Do cech dodatkowych można zaliczyć prędkość nagrywania do 400 kl./s w rozdzielczości D1 z kompresją H.264 oraz możliwość podłączenia czterech monitorów do jednego urządzenia.

Monitory

Grundig rozwija również swoją ofertę w zakresie płaskich monitorów przeznaczonych do systemów CCTV. Profesjonalna linia monitorów powstała dzięki wieloletniemu doświadczeniu firmy w projektowaniu i produkcji telewizorów przeznaczonych dla konsumentów indywidualnych.

Linia płaskich monitorów TFT wykorzystuje technologię podświetlania LED, dzięki czemu odtwarzane obrazy cechują się wysokim kontrastem i wierną reprodukcją barw.

Podświetlanie w technologii LED znacząco różni się od tradycyjnego podświetlania CCFL. Zapewnia większą skalę barw i pozwala ukazać szersze spektrum kolorów, lepiej odzwierciedlające realny obraz.

Połączenie wymienionych funkcji wpływa znacząco na kontrast obrazu.

Fot. 6. Monitor LCD 23.6" z podświetleniem LED, model GML-2430M

Fot. 7. Extender sygnału ethernet po kablu koncentrycznym, model GTI-F0022C

W swojej ofercie Grundig posiada monitory o wielkości od 10 do 24 cali, umożliwiające pełną operacyjność 24/7 z zachowaniem niskiego poboru energii.

Transmisja i akcesoria uzupełniające

W skład urządzeń służących do transmisji obrazu i danych wchodzą extendery transmisji sygnałów wizyjnych oraz adaptery zasilania PoE wraz z odpowiednimi konwerterami i wzmacniaczami. Transmisja danych z wykorzystaniem technologii VDSL2 na odległość od 200 do 1000 metrów nie napotyka już żadnych przeszkód, podobnie jak konwertowanie mediów czy też interfejsów z HD-SDI na HDMI, co umożliwia bezpośrednie podłączenie kamery do monitora. Właściwie dobrane komponenty torów transmisyjnych zapewniają przekaz obrazu najwyższej jakości nawet przy dużych dystansach. Wszystkie urządzenia są zgodne ze światowymi standardami i normami.

Bogata oferta własnych komponentów ułatwiających proces montażu, takich jak uchwyty, obudowy oraz adaptery, znacząco wpływa na szybkość i wygodę instalacji systemu. Wysoka jakość materiałów użytych do produkcji akcesoriów zapewnia ich niezawodność i estetykę na najwyższym poziomie. Również oferta C&C Partners w zakresie kabli instalacyjnych koncentrycznych oraz skrętkowych, obiektywów, zasilaczy i obudów uzupełniająca listę akcesoriów firmy Grundig pozwala na przyśpieszenie i usprawnienie procesu projektowania i instalowania kompletnego systemu CCTV.

Dostarczamy produkty najwyższej jakości i w taki sposób, aby współpracujący z nami Partnerzy mieli pewność, że wdrażany system nadzoru bezpieczeństwa będzie zawsze niezawodnie spełniał swoje zadanie.

Konrad Staniewski

kierownik produktu Grundig CCTV
e-mail: k.staniewski@ccpartners.pl
www.ccpartners.pl
www.b2b-ccpartners.pl

Wysokiej jakości detekcja termowizyjna, PTZ i nadzór HDTV w jednym

Agata Majkucińska

Axis wprowadza na rynek dualną kamerę sieciową PTZ przeznaczoną do zastosowań specjalnych, umożliwiającą całodobową obserwację dozorowanego terenu oraz wykrywanie, rozpoznawanie i identyfikację zbliżających się obiektów. We wspólnej obudowie umieszczone są dwie kamery sieciowe – kamera termowizyjna, pracująca w widmie głębokiej podczerwieni, umożliwiająca wykrywanie zbliżających się obiektów, oraz kamera HDTV z obiektywem zmiennoogniskowym, pracująca w widmie optycznym, umożliwiająca rozpoznawanie i identyfikację obiektów wykrytych przez kamerę termowizyjną

Fot. 1. AXIS Q87 – Detekcja termiczna i kamera HDTV z opcją PTZ w jednym

Axis Communications wprowadza na rynek serię dualnych kamer sieciowych AXIS Q87-E przeznaczonych do pracy w trudnych warunkach klimatycznych, stanowiących pod względem funkcjonalnym połączenie klasycznych kamer PTZ z kamerami termowizyjnymi. Podstawową zaletą wyróżniającą te urządzenia i odróżniającą je od konkurencyjnych produktów jest integracja funkcji wykrywania obiektów za pomocą kamery termowizyjnej z funkcją ich rozpoznawania i identyfikacji za pomocą kamery optycznej o wysokiej rozdzielczości, wyposażonej w obiektyw zmiennoogniskowy. Możliwe jest także zastosowanie oświetlaczy

Fot. 2. AXIS 87-E z funkcją PTZ wytwarza dwa strumienie wizyjne, z kamery optycznej i z kamery termowizyjnej

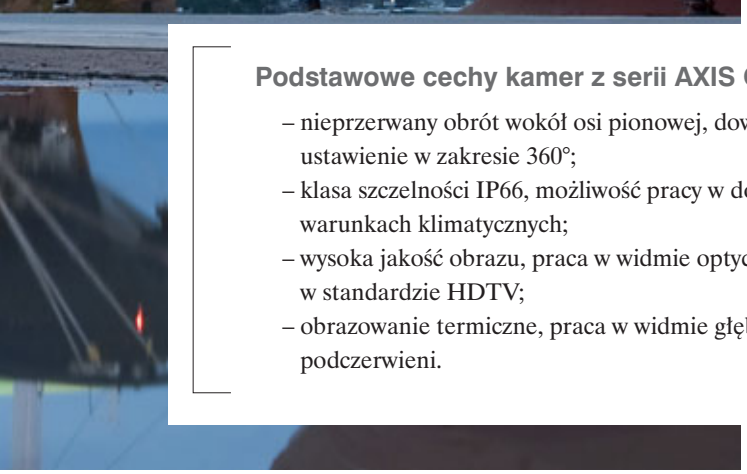
pracujących w widmie płytkiej podczerwieni, obracających się wraz z tymi kamerami, dzięki którym kamera optyczna może pełnić swoje funkcje w nocy lub w złych warunkach oświetleniowych.

Zespół wyżej wymienionych urządzeń stanowi zintegrowaną całość i jest umieszczony na uchylno-obrotowej głowicy przystosowanej do pracy w trudnych warunkach klimatycznych. Już w marcu 2012 roku takie kamery zostały zaprezentowane na targach ISC West w Las Vegas, gdzie wzbudziły duże zainteresowanie wśród projektantów i instalatorów.

Jak już wspomniano, dualna kamera sieciowa AXIS Q87-E jest umieszczona na głowicy uchylno-obrotowej, dzięki czemu oba jej składniki, to znaczy zarówno kamera termowizyjna, jak i klasyczna kamera HDTV, jednocześnie zmieniają swoje położenie. Umożliwia to prowadzenie obserwacji w dwóch różnych widmach, termicznym i optycznym, co z kolei umożliwia wykorzystanie kamer dualnych przez dwadzieścia cztery godziny na dobę, niezależnie od warunków oświetleniowych i pogodowych. Dzięki temu kamery dualne znajdują zastosowanie w obserwacji obszarów o znaczeniu krytycznym, takich jak nabrzeża portowe, granice wydzielonych terenów przemysłowych i wojskowych, granice państw etc.

Do serii kamer AXIS Q87-E należą dwa modele:

– AXIS Q8721-E, której część optyczna pracuje w standardzie HDTV 1080i i jest wyposażona w obiektyw zmiennoogniskowy o krotności x10, zaś część termiczna wytwarza obraz o rozdzielczości 384×288 pikseli;
– AXIS Q8722-E, której część optyczna nie różni się od zastosowanej w modelu Q8721-E, zaś część termiczna ma rozdzielczość VGA (640×480).



Podstawowe cechy kamer z serii AXIS Q87-E

– nieprzerwany obrót wokół osi pionowej, dowolne ustawienie w zakresie 360°;
– klasa szczelności IP66, możliwość pracy w dowolnych warunkach klimatycznych;
– wysoka jakość obrazu, praca w widmie optycznym w standardzie HDTV;
– obrazowanie termiczne, praca w widmie głębokiej podczerwieni.

Fot. 3. AXIS Q87-E pozwala na wykrywanie, rozpoznawanie i identyfikację obiektów z użyciem pojedynczego urządzenia

Detekcja, rozpoznawanie, identyfikacja

W kamerach z serii AXIS Q87-E wykorzystane zostały najnowsze osiągnięcia technologiczne z dziedziny telewizji dozorowej oraz termowizji. Każda ze zintegrowanych kamer z serii AXIS Q87-E stanowi połączenie nowoczesnej kamery termowizyjnej z kamerą pracującą w widmie optycznym, wyposażoną w obiektyw zmiennoogniskowy o krotności x10, przy czym ruchy obu tych kamer są zsynchronizowane dzięki umieszczeniu ich we wspólnej obudowie, na głowicy uchylno-obrotowej. Zastosowana tu kamera termowizyjna najnowszej generacji zapewnia skuteczne wykrywanie zbliżających się obiektów w dowolnych warunkach oświetleniowych i pogodowych, nawet w zupełniej ciemności, zaś kamera pracująca w widmie optycznym umożliwia rozpoznawanie i identyfikację tych obiektów, także nocą, z wykorzystaniem zintegrowanych oświetlaczy pracujących w widmie płytkiej podczerwieni.

Oba modele są podłączane do sieci Ethernet i mogą być zasilane za pomocą pojedynczego kabla, który może być wykorzystany także do zasilania całego zintegrowanego zespołu urządzeń.

Kompresja H.264 oraz wytwarzanie kilku strumieni wizyjnych

Obie kamery, termowizyjna i optyczna, mogą wytwarzać kilka niezależnych strumieni wizyjnych z kompresją H.264. Strumienie wizyjne mogą różnić się rozdzielczością, stopniem kompresji i jakością obrazów w zależności od pasma sieciowego dostępnego podczas transmisji danych.

Wykrywanie obiektów przez kamerę termowizyjną jest szczególnie istotne w nocy, gdy brakuje jakiegokolwiek oświetlenia obserwowanego terenu, oraz w bardzo złych warunkach pogodowych. Aby poprawić skuteczność wykrywania obiektów w części termicznej, można zastosować jeden z czterech rodzajów obiektywów.

Z kolei pracująca w widmie optycznym kamera HDTV umożliwia rozpoznanie i identyfikację wykrytych obiektów, przy czym w nocy można skorzystać z dodatkowych promienników podczerwieni o zasięgu dochodzącym do 100 metrów.

Praca w dowolnych warunkach klimatycznych

Kamery z serii AXIS Q87-E zostały zaprojektowane z myślą o wykorzystaniu ich w systemach dozorowych o znaczeniu krytycznym, instalowanych na zewnątrz budynków, pracujących w dowolnych warunkach klimatycznych. Z tego względu obudowy tych kamer mają klasę szczelności IP66 i są odporne na wpływ zanieczyszczeń i strumieni wody o dużym ciśnieniu, na jakie mogą być narażone w trudnych warunkach eksploatacyjnych. Kamery z serii AXIS Q87-E mogą pracować w temperaturze od –30 °C do +45 °C. Obie kamery składowe, termowizyjna i optyczna, są połączone z przełącznikiem sieciowym znajdującym się wewnątrz obudowy, dzięki czemu cały ten zespół urządzeń łączy się z siecią Ethernet za pośrednictwem pojedynczego kabla.

Jak stwierdził Fredrik Nilsson, dyrektor generalny Axis Communications, w chwili obecnej kamery z serii AXIS Q87-E stanowią najlepsze z dostępnych na światowym rynku rozwiązań z dziedziny wizyjnych systemów dozorowych przeznaczonych do zastosowań specjalnych, o znaczeniu krytycznym. Kamera termowizyjna pozwala na wykrywanie zbliżających się obiektów, zaś kamera HDTV umożliwia sprawdzenie, czy dana osoba lub pojazd ma prawo przekraczać granice obserwowanego obszaru. Umieszczenie kamery termowizyjnej i kamery optycznej na wspólnej głowicy uchylno-obrotowej pozwala na synchronizację obrazów wytwarzanych przez te kamery i tym samym umożliwia skuteczną ochronę granic państwowych oraz ścisły nadzór nad obiektami przemysłowymi i wojskowymi praktycznie w każdych warunkach oświetleniowych i pogodowych. Zespolone kamery termowizyjne i optyczne są też użytecznymi narzędziami dla osób dbających o bezpieczeństwo publiczne w obiektach cywilnych.

Oba modele kamer z serii AXIS Q87-E mogą wykonywać nieprzerwany ruch obrotowy wokół osi pionowej, czyli mogą przyjmować dowolne azymutalne ustawienie w zakresie 360°, i mogą być pochylane wokół osi poziomej w zakresie od +45° do –20°. Można regulować ich położenie z dokładnością do 0,02°. Obie kamery mają klasę szczelności IP66 i mogą pracować w zakresie temperatur od –30°C do +45°C. Są wyposażone w gniazdo, w którym można umieścić kartę pamięci SD/SDHC w celu lokalnego zapisu materiału wizyjnego.

Dzięki rozwijanemu przez firmę Axis programowi Application Development Partner oraz wprowadzeniu na rynek oprogramowania AXIS Camera Station, planując wykorzystanie dowolnej z sieciowych kamer dualnych z serii AXIS Q87-E, można skorzystać z największej dostępnej na świecie przemysłowej bazy oprogramowania systemowego.

Kamery z serii AXIS Q87-E współpracują z oprogramowaniem dostępnym w ramach AXIS Camera Application Platform, z czego mogą skorzystać twórcy aplikacji w celu stworzenia nowych funkcji użytkowych w swoich systemach.

Agata Majkucińska
Axis Communications

Łatwa instalacja w warunkach terenowych

Aby ułatwić pracę instalatorom i konserwatorom, firma Axis wprowadziła na rynek monitor instalacyjny AXIS T8414. Jest to przenośne, zasilane bateriami urządzenie, które można podłączyć bezpośrednio do kamery i wyświetlać na nim obraz w miejscu instalacji. Dzięki temu regulacja kamery jest znacznie prostsza niż w przypadku użycia przenośnego lub stacjonarnego komputera PC. Urządzenie AXIS T8414 jest łatwe w obsłudze dzięki zastosowaniu ekranu dotykowego.

Teraz w Polsce

Axis Communications' Academy

Budowanie kompetencji w dziedzinie sieciowych systemów wizyjnych

Liczba klientów i sukces Twojej firmy zależą od tego, czy dysponujesz najbardziej aktualną i wszechstronną wiedzą w branży. Dzięki szkoleniom w ramach Axis Communications' Academy łatwiej być o krok do przodu przed konkurencją – wiedza z dziedziny sieciowych systemów wizyjnych jest w zasięgu ręki.

Akademia oferuje bogactwo informacji, które umożliwiają budowanie kompetencji w każdej części łańcucha produktów – od interaktywnych narzędzi do projektowania systemów, praktycznych instrukcji „krok po kroku" i specjalistycznych seminariów internetowych po szkolenia stacjonarne i programy certyfikacyjne. Tę wiedzę przekazują przeszkoleni specjaliści Axis. Jest ona dostępna w każdej chwili, w każdym miejscu i w ojczystym języku.

Gdy źródłem Twojej wiedzy jest firma, która opracowała pierwsze sieciowe systemy wizyjne i nadal ustanawia branżowe standardy w zakresie innowacji, świadomi klienci doceniają Twoje doświadczenie co przynosi w konsekwencji wymierne korzyści.

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

Axis Communications' Academy - globalne centrum wiedzy z dziedziny sieciowych systemów wizyjnych

AXIS COMMUNICATIONS

Rozdzielczość i czułość kamer IP

System IP CCTV marki NOVUS dla liczarni pieniędzy i punktów kasowych

Patryk Gańko

Podczas wielokrotnych rozmów z instalatorami na temat koncepcji systemu telewizji dozorowej (CCTV) w danym obiekcie próbowałem poznać kryteria techniczne, którymi kierowano się przy wyborze kamer. Najczęściej powtarzającymi się parametrami były rozdzielczość obrazu oraz czułość kamer, czyli ich zdolność do pracy w trudnych warunkach oświetleniowych. Pozostałe parametry schodziły na dalszy plan i pojawiały się tylko w kontekście szczegółowych wymagań inwestora lub istotnych zapisów w specyfikacji zamówienia

Weryfikacja pracy systemu nadzoru wizyjnego w obiekcie wskazuje, że najczęściej stosowaną konfiguracją są ustawienia domyślne, co oznacza, że wszystkie zaawansowane funkcje nie są traktowane priorytetowo. Co więcej, parametry rozdzielczości i czułości są dla instalatora trudne do zweryfikowania i wymagają nie tylko dużego doświadczenia, ale także solidnego zaplecza, potrzebnych do oceny prawdziwości danych katalogowych w tym zakresie. Właśnie dlatego na łamach niniejszego artykułu chciałbym poruszyć problem rozdzielczości na przykładzie kamer IP w często stosowanym rozwiązaniu – urządzeniu do rozpoznawania banknotów w punktach kasowych oraz liczarniach pieniędzy. Dodatkowo chciałbym odnieść się do drugiego parametru – czułości kamer IP w porównaniu z czułością powszechnie stosowanych dotychczas kamer analogowych.

Rozpoznawanie banknotów może być realizowane na dwa sposoby:

– rozpoznawanie jedynie nominalnej wartości banknotów,
– rozpoznawanie nominalnej wartości banknotów oraz odczytywanie znaków alfanumerycznych na banknotach (numerów seryjnych).

Bez wątpienia drugi sposób jest trudniejszy, ale niejako „po drodze" rozwiązuje pierwszy wspomniany problem. W przypadku systemu analogowego w praktycznych aplikacjach możliwe było tylko rozpoznawanie wartości banknotów. Nie można było stworzyć systemu umożliwiającego odczyt numerów seryjnych na banknotach ze względu na zbyt małą liczbę pikseli przypadającą na odczytywany znak. Dopiero wprowadzenie kamer IP o dużej rozdzielczości pozwoliło rozpoznawać numery seryjne poszczególnych banknotów.

Do rozpoznania znaku o szerokości 2 mm (standardowa, przybliżona szerokość znaków umieszczanych na banknotach) wymaganych jest minimum 6 pikseli matrycy. W przypadku kamer NVIP-2DN5001C-1P (*http://www.novuscctv.pl/pl/node/7615*) z przetwornikiem obrazu CMOS 2.0 Mpx o liczbie efektywnych pikseli 1920 (H)×1080 (V) szerokość obserwowanego obszaru nie powinna przekraczać 640 mm. Z proporcji obrazu 16:9, typowej dla kamer Full HD, wynika, że wysokość takiego obszaru wyniesie zaledwie 360 mm. Obszar o wymiarach 640×360 mm pokrywa się ze standardowym obszarem pracy liczarza lub kasjera, w obrębie którego operuje on banknotami. Aby zapewnić pełny ogląd sytuacji oraz ustalić kierunek przekazywania pieniędzy do strefy rozpoznawania numerów seryjnych, można uzupełnić punkt kamerowy o dodatkową kamerę o szerszym polu widzenia, ale już bez możliwości rozpoznawania numerów seryjnych.

Jeszcze lepsze rezultaty można osiągnąć, używając kamer o rozdzielczości 5 Mpx. Zastosowanie prototypowego modelu o rozdzielczości 2592 (H)×1944 (V) daje większy obszar, na którym rozpoznawane są numery seryjne. Dostępny obszar ma 850 mm szerokości oraz 640 mm wysokości.

Dodatkowym utrudnieniem przy rozpoznawaniu numerów seryjnych banknotów 200-złotowych jest zmienna wielkość znaków alfanumerycznych widocznych na każdym z tych banknotów.

Dużą zaletą kamery NVIP-2DN5001C-1P jest duża poklatkowość wynosząca 25 obrazów/s. Ma to ogromne znaczenie, ponieważ proces wymiany, przekazywania i przeliczania

Fot. 1. Rozpoznanie numerów seryjnych banknotów, obszar rozpoznania: 640×360 mm, kamera NVIP-2DN5001C-1P

Fot. 2. Rozpoznanie numerów seryjnych banknotów, obszar rozpoznania: 850×640 mm, kamera 5 Mpx

Fot. 3. Pogorszenie jakości obrazu i zdolności do rozpoznawania numerów w przypadku natężenia oświetlenia wynoszącego 200 luksów

banknotów cechuje się dużą dynamiką. Konieczne jest więc tworzenie i rejestracja strumienia wizyjnego w trybie *live*. Kamery o rozdzielczości 5 Mpx nie spełniają tego warunku, gdyż podczas pracy przy najwyższej rozdzielczości wytwarzają 10 obrazów/s. Prawdopodobieństwo odczytu numerów seryjnych będzie w takich warunkach mniejsze niż w przypadku zastosowania kamery Full HD.

Niebagatelny wpływ na poprawność odczytu ma odpowiednie natężenie oświetlenia na zadanym obszarze. Z przeprowadzonych testów wynika, że w przypadku poziomu oświetlenia przekraczającego 600 luksów czas ekspozycji jest tak krótki, że obraz jest wystarczająco ostry i ma odpowiedni kontrast. Przy słabszym oświetleniu kontrastowość maleje. Aby zapewnić rozpoznanie numerów seryjnych banknotów, należy zmniejszyć obszar rozpoznania poprzez zwiększenie ogniskowej obiektywu lub zmianę położenia kamery.

Kolejnym czynnikiem, który ma wpływ na skuteczność rozpoznania znaków alfanumerycznych, jest odpowiedni dobór obiektywu. Ze względu na dużą rozdzielczość wynikowego obrazu konieczne jest stosowanie precyzyjnie wykonanych obiektywów. Należy wziąć pod uwagę osiowość montażu obiektywu, stabilność pierścienia mocującego oraz rosnące aberracje układu optycznego obiektywu na krańcach pola widzenia. Ten ostatni parametr nie jest podawany w standardowych specyfikacjach obiektywów, więc – by go poznać – należy zasięgnąć informacji bezpośrednio u producenta. Ważne jest też dobranie długości ogniskowej tak, by maksymalnie ograniczyć pracę na krańcach pola widzenia systemu optycznego.

Zamieszczone w artykule rysunki ilustrujące problematykę rozpoznawania znaków alfanumerycznych są dostępne na stronie *www.novuscctv.com*. Zapoznanie się z nimi umożliwia adekwatną ocenę jakości systemu optycznego. Oprócz rysunków dostępne są także zdjęcia z opisami i materiał filmowy odnoszący się do wątków poruszanych w artykule. Istnieje wiele mitów dotyczących czułości kamer IP. Czułość, czyli minimalne oświetlenie, jakie jest potrzebne, aby kamera wygenerowała użyteczny obraz, jest tym parametrem kamery, który trudno wiarygodnie ocenić. Wynika to z faktu, że producenci nie wyznaczyli standardowych metod pomiaru czułości przetworników i podają minimalne wartości oświetlenia dla różnych poziomów sygnału wizyjnego i różnych czasów ekspozycji. Nie wiadomo także, czy pomiary dotyczą poziomu oświetlenia przetwornika czy poziomu oświetlenia sceny obserwowanej przez kamery z układem optycznym. Z tego powodu dane katalogowe są w zasadzie nieporównywalne.

W powszechnej opinii technologia przetworników obrazu CMOS stosowana w kamerach megapikselowych ustępuje pod względem czułości technologii CCD. Rzeczywiście – tak było w przypadku starszych generacji kamer z przetwornikami CMOS, jednakże rozwój technologii CMOS pozwolił zniwelować te różnice. Kamery Full HD marki NOVUS można z powodzeniem stosować w trudnych warunkach oświetleniowych i zastępować nimi stosowane dotychczas kamery analogowe z przetwornikami CCD.

Pod linkiem *http://www.novuscctv.pl/pl/node/9327* można znaleźć materiały filmowe porównujące czułość kamer analogowych z czułością kamer Full HD i czułością standardowych kamer IP. Cztery ww. kamery zostały zainstalowane wewnątrz komory z płynnie regulowanym poziomem oświetlenia i obserwowały tablicę testową z przemieszczającą się strzałką. Testy przeprowadzono przy różnych rodzajach oświetlenia (światło białe i podczerwone) oraz przy włączonej funkcji WDR. Załączone materiały jednoznacznie wskazują na porównywalność technologii CCD i CMOS pod względem czułości.

Zastosowanie kamer IP w systemach kasowych oraz w liczarniach pieniędzy pozwala na uniknięcie lub polubowne rozwiązanie wielu spornych kwestii zaistniałych podczas obsługi klientów. Wysoka rozdzielczość zapisywanego materiału pozwala na jednoznaczne rozstrzygnięcie wątpliwych przypadków. Stosując kamery IP, można zapewnić rozpoznawalność banknotów na relatywnie dużym obszarze, który obejmuje całą przestrzeń wokół punktu kasowego. Dodatkowo monitorowanie numerów seryjnych banknotów usprawnia proces eliminowania fałszywych banknotów i pozwala na wykrywanie miejsc wprowadzania ich do obiegu.

Patryk Gańko
AAT Holding

Nowa centrala alarmowa i klawiatura z serii POWER

DSC

PC1404
Centrala alarmowa

- Przeznaczona do stosowania w mieszkaniach, sklepach, biurach itp.
- 4 - 8 linii dozorowych
- Do 4 klawiatur w systemie
- Wbudowany dialer telefoniczny
- Obsługa do 4 numerów telefonów
- 1 podsystem
- Rejestr 128 zdarzeń
- 39 kodów użytkownika
- Elastyczna konfiguracja

PC1404 RKZ
8-liniowa klawiatura LED

- Kompatybilna z centralami PC1404, PC1616, PC1832, PC1864
- Nowoczesny wygląd
- Podświetlone przyciski ułatwiające obsługę
- 4 programowalne przyciski funkcyjne
- Zacisk linii klawiaturowej
- Podwójne przyciski Pożar, Pomoc, Panika
- Podwójne zabezpieczenie antysabotażowe przed otwarciem lub oderwaniem od ściany
- Obsługa 1 podsystemu

Seria POWER to funkcjonalne i niezawodne rozwiązania, dopasowane do indywidualnych potrzeb użytkowników. Wszystkie urządzenia w ramach serii są ze sobą kompatybilne i umożliwiają dowolną konfigurację systemu alarmowego.

Wyłączny dystrybutor produktów DSC w Polsce:

AAT

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

Oprogramowanie F-Link
dla systemu JABLOTRON 100

Piotr Panek

Nowy system alarmowy marki JABLOTRON łączy w sobie różne rozwiązania służące zabezpieczeniu obiektu, a dzięki wszechstronnym możliwościom konfiguracyjnym pozwala na realizację funkcji inteligentnego domu. Zanim jednak użytkownik będzie mógł osiągnąć efekt końcowy instalacji, potrzebne są narzędzia umożliwiające jej przygotowanie. Jednym z nich jest oprogramowanie F-Link

Podstawowym celem twórców tego oprogramowania była jego prostota i intuicyjność obsługi. Obsługę oprogramowania opracowano w sposób przypominający proces wykonywania i uruchamiania instalacji. Ustawień systemu dokonuje się za pomocą kolejnych zakładek, przechodząc od ustawień podstawowych do bardziej szczegółowych, powiązanych z konkretnym fragmentem pracy systemu. Przycisk *Więcej* odsłania zaawansowane funkcje w każdej z zakładek. Dla każdego fragmentu ustawień dostępna jest pomoc w postaci wyskakującej podpowiedzi.

Wspomniane zakładki są następujące:

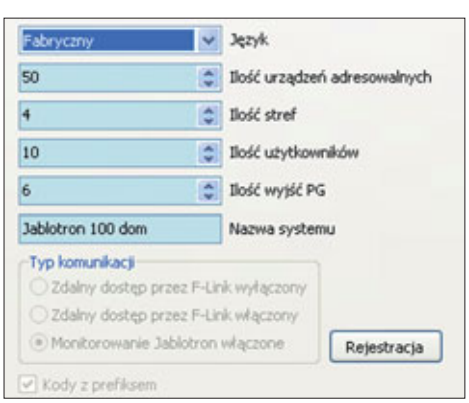
– Podstawowe ustawienia

Tu określa się schemat systemu, liczbę urządzeń adresowalnych, stref, użytkowników oraz wyjść do sterowania automatyką budynkową. Zadeklarowanie tych danych na początku ułatwia dalszą konfigurację całości. Jeśli na przykład zadeklarujemy pięćdziesiąt urządzeń adresowalnych i pięć stref, to w kolejnych oknach programu pojawi się tylko taka ich liczba.

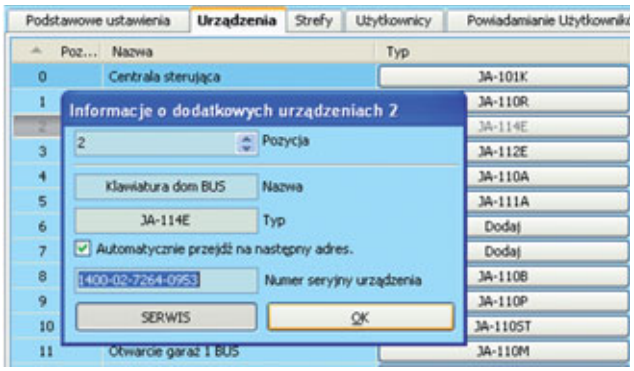
W tej zakładce należy wybrać sposób zdalnego komunikowania się z centralą systemu. Możliwe jest wyłączenie tej funkcji, włączenie jej tylko dla komunikacji poprzez program F-Link oraz włączenie pełnej komunikacji przez serwer firmy JABLOTRON. Ta ostatnia opcja wymaga rejestracji na stronie *www.jablonet.net*, pozwala na obsługę zdalną poprzez stronę WWW i aplikacje mobilne dla współczesnych telefonów.

– Urządzenia

W tej zakładce przypisuje się adresy systemowe urządzeniom pracującym w systemie. Zwykle na pojedyncze urządzenie przypada jeden adres. Fabrycznie adres numer jeden jest przypisany do centrali sterującej. Po naciśnięciu przycisku *Dodaj* otwiera się niewielkie okno, w którym można zdefiniować i zaadresować nowe urządzenie. Dokonuje się tego na dwa sposoby. Pierwszy polega na wpisaniu indywidualnego numeru urządzenia. Drugi – na aktywowaniu sabotażu dodawanego urządzenia (rys. 2). W momencie aktywacji sabotażu system automatycznie rozpoznaje typ urządzenia (można wprowadzić własny opis). Dla większej przejrzystości przy numerach adresów urządzeń bezprzewodowych pojawia



Rys. 1. Podstawowe ustawienia instalacji



Rys. 2. Adresowanie urządzeń

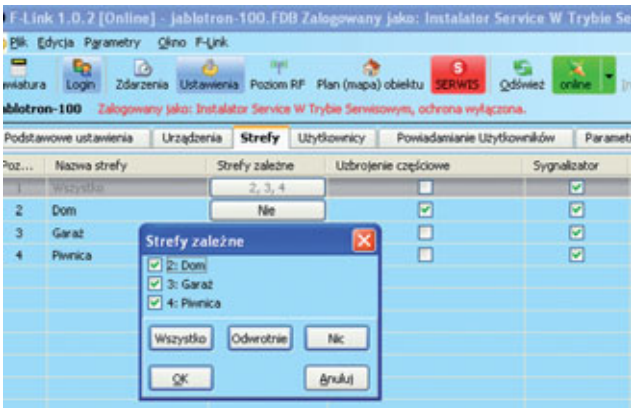
się symbol anteny. Po zaadresowaniu urządzeń można dokonywać indywidualnych ustawień nastaw dla każdego z nich. Robi się to po naciśnięciu przycisku *Ustawienia wewnętrzn*e, w wyniku czego otwiera się okno ustawień pojedynczego elementu. W przypadku klawiatury można przypisać funkcje segmentom sterującym, określić, w jaki sposób będzie ona informować użytkownika o stanie systemu, oraz dopasować zakres jej pracy do wymogów instalacji (rys. 3). Parametry znajdujące się w tym oknie są odmienne dla różnych grup urządzeń, co ułatwia pracę osobie programującej. W starszych rozwiązaniach wiele funkcji było ustawianych za pomocą fizycznego przełącznika na urządzeniu, co ograniczało możliwości wyboru rodzajów pracy urządzenia oraz wymagało niejednokrotnie większego nakładu pracy przy uruchamianiu systemu.

W tej zakładce określa się również przydział do strefy, opcje pamięci alarmu, opcje nadzoru sygnału radiowego oraz blokowania pojedynczego elementu. Pokazywana jest też informacja o ewentualnych usterkach urządzenia o konkretnym adresie.

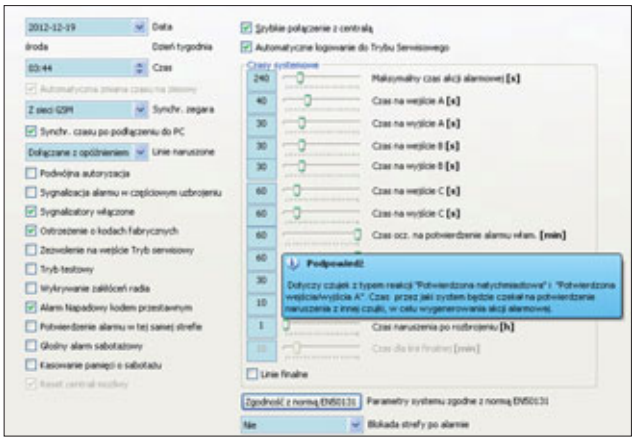
– Strefy i Wyjścia programowalne

W tych zakładkach definiowane są strefy: ich nazwy oraz funkcje. Każda ze stref jest obsługiwana oddzielnie, z wyjątkiem zdefiniowanych jako zależne (rys. 4). W takiej sytuacji włączenie dozoru jednej strefy powoduje automatyczne włączenie dozoru innych stref, zdefiniowanych jako zależne. Zazwyczaj pojedyncza strefa jest powiązana z segmentem sterującym na klawiaturze. Załączenie dozoru danej strefy następuje po przyciśnięciu czerwonego przycisku na klawiaturze, a wyłączenie dozoru – zielonego przycisku. Do wyłączenia dozoru konieczna jest autoryzacja za pomocą kodu lub karty RFID. Możliwe jest zdefiniowanie strefy wewnętrznej nocnej, obejmującej jedynie tę część obiektu, którą należy dozorować nocą podczas przebywania w nim domowników (np. okna, parter, piwnice). Ten rodzaj

Rys. 3. Ustawienia wewnętrzne klawiatury



Rys. 4. Strefy zależne



Rys. 8. Parametry

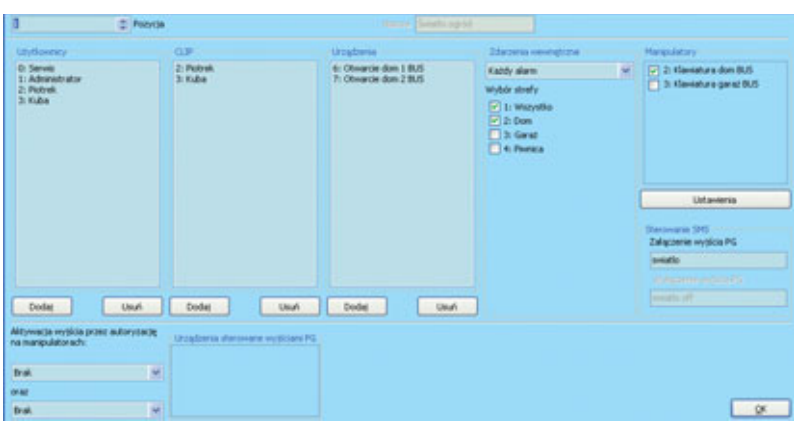
załączenia jest sygnalizowany kolorem pomarańczowym na segmencie powiązanym z daną strefą. Można również zdefiniować załączanie i wyłączanie dozoru określonej strefy (stref) według zdefiniowanego harmonogramu czasowego. Metoda ta ma zastosowanie do obiektów, w których czas ochrony jest sprecyzowany.

W przypadku wyjść programowalnych należy określić nazwę każdego z nich, typ i logikę działania. Następnie, po naciśnięciu przycisku *Funkcje PG*, określa się, kto będzie mógł aktywować dane wyjście i w jaki sposób (np. przez klip, komendę lub SMS). Załączenie wyjścia może nastąpić po aktywacji dowolnej czujki lub segmentu klawiatury albo po zdarzeniu systemowym (rys. 5).

– *Użytkownicy* i *Powiadomienia użytkowników*

W pierwszej z tych zakładek należy zdefiniować wszystkich użytkowników systemu i wprowadzić używane przez nich numery telefonów. Wprowadzenie numerów telefonów nie jest wprawdzie obowiązkowe, ale umożliwia szybkie przesłanie informacji i zdalną komunikację (każda z central JABLOTRON 100 jest fabrycznie wyposażona w komunikator GSM). Osobom obsługującym system należy przydzielić właściwe uprawnienia oraz nadać możliwość obsługi wybranych stref i wyjść programowych. Pracownicy serwisu mają dostęp do wszystkich ustawień systemu. Administratorzy mogą obsługiwać system i nadawać uprawnienia użytkownikom. Użytkownicy posiadają uprawnienia określone przez administratorów i nie mogą sami decydować o funkcjonalności swojego kodu (rys. 6).

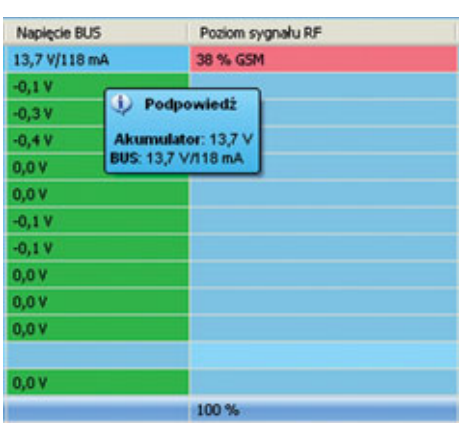
W zakładce *Powiadomienia użytkowników* wprowadza się precyzyjne ustawienia dotyczące raportów wysyłanych przez centralę alarmową. Ułatwieniem dla programującego jest pogrupowanie raportów w taki sposób, że nie trzeba każdego zdarzenia zaznaczać oddzielnie. W zależności od potrzeb należy zaznaczyć powiadamianie w formie SMS-a lub wiadomości głosowej. Można również oddzielnie wybrać informowanie o włączeniach i wyłączeniach dozoru, przesyłanie zdjęć z kamer sprzężonych z systemem oraz przesyłanie informacji dotyczących technicznych aspektów pracy systemu. Każdy z użytkowników otrzymuje raporty dotyczące tylko tych stref i wyjść programowalnych, które zostały mu przypisane. W celu sprawdzenia właściwej formy raportu należy użyć przycisku *Test* (rys. 7).



Rys. 5. Funkcje wyjść programowalnych

Rys. 6. Użytkownicy

Rys. 7. Raporty



Rys. 9. Diagnostyka

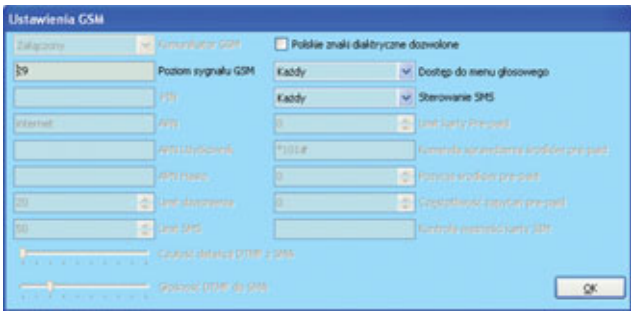
– *Parametry* i *Diagnostyka*

W pierwszej zakładce dokonuje się ustawień dotyczących pracy centrali alarmowej. Z lewej strony okna pokazane są najistotniejsze parametry. Niektóre z nich określa się globalnie (dla całego systemu) i szczegółowo dopasowuje do konkretnych urządzeń o zadanych adresach. Dzięki temu instalator może szybko wprowadzić ustawienie, które jest dla niego najistotniejsze. Po prawej stronie okna można określić czasy systemowe. W celu uproszczenia nastaw zastosowano specjalne suwaki. Jeżeli czujki instalowane są w trudnym środowisku, można skorzystać z opcji redukcji fałszywych alarmów. W tym celu wykorzystuje się funkcję powtórnego naruszenia danej strefy lub potwierdzenia z innej strefy alarmowej. W dolnej części okna można również włączyć automatyczne dostosowanie ustawień do normy EN50131 (rys. 8).

JABLOTRON 100 to system magistralowy, w którym występuje połączenie dwóch torów transmisji sygnału. Pierwszym z nich jest czterożyłowa magistrala, a drugim – tor radiowy. Przy maksymalnej liczbie urządzeń adresowalnych 120 oraz nieograniczonej liczbie urządzeń bez adresu konieczne było zastosowanie pełnej kontroli wszystkich elementów. Oprócz znanego z poprzednich modeli systemów analizatora widma sygnału radiowego dodano zakładkę *Diagnostyka*. Przez cały czas sprawdzane są parametry magistrali oraz sygnału radiowego i komunikacji LAN/GSM. Każda usterka lub niezgodność z właściwym stanem są pokazywane na ekranie (rys. 9).

– *Ustawienia komunikatorów*

Każda z central tej serii systemu JABLOTRON 100 posiada wbudowany komunikator GSM, natomiast największa z nich jest jeszcze wyposażona w łączność LAN. Oba komunikatory centrali umożliwiają pełne raportowanie zdarzeń oraz zdalną obsługę systemu. Wybierając komunikator GSM, można zobaczyć poziom sygnału sieci oraz określić parametry pracy dla tej komunikacji. Do ważniejszych należą możliwości zapobiegania wysyłaniu nadmiernej liczby SMS-ów i wykonywaniu zbyt dużej liczby połączeń. Instalator może dokładnie określić, ile wiadomości SMS może wysłać centrala w danym dniu i ile wykonać połączeń. Obydwa komunikatory umożliwiają również wprowadzenie ustawień dotyczących łączności z systemem monitoringu (rys. 10).



Rys. 10. Ustawienia GSM

Opisane powyżej zakładki są elementami oprogramowania F-Link dla systemów serii JABLOTRON 100. Artykuł ten ma na celu przybliżenie czytelnikom omawianego oprogramowania i pokazanie, jak za jego pomocą zaprogramować centrale nowego systemu.

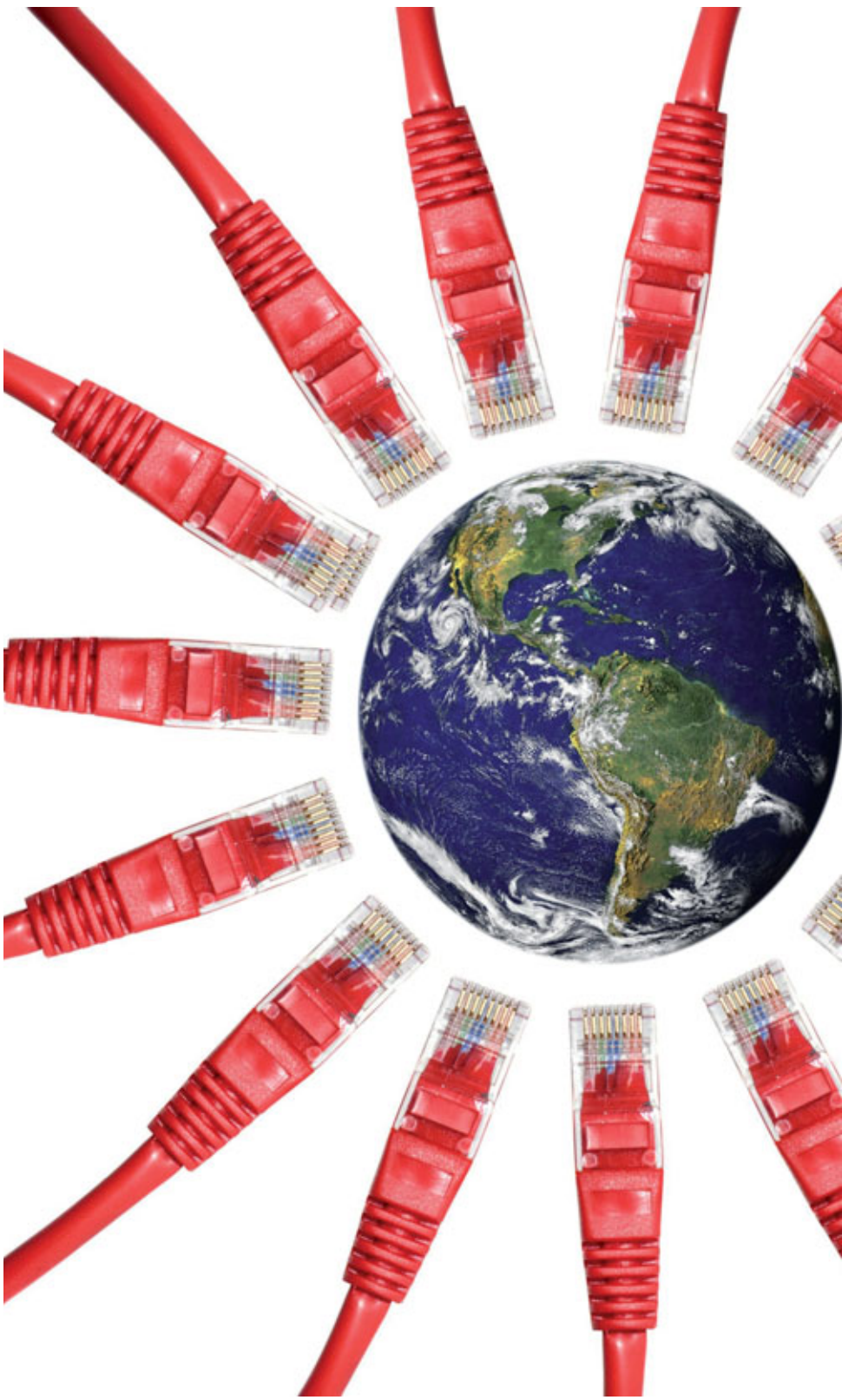
Piotr Panek
JABLOTRON ALARMS

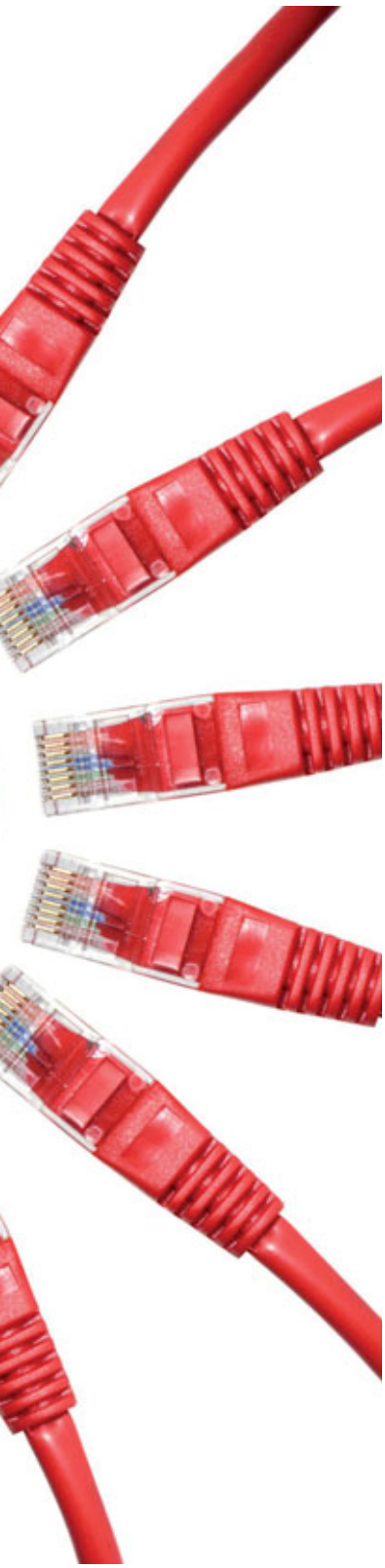
Interkom dla każdego!

Bezserwerowy system interkomowy Pulse

Adam Gregorczyk

Nie rzucamy bynajmniej populistycznego hasła – proponujemy ekonomiczny system łączności i rozwiązania techniczne do współczesnych systemów VoIP





System Pulse firmy STENTOFON został zaprojektowany jako rozwiązanie bezserwerowe. Dzięki temu inwestor nie musi kupować kosztownego serwera VoIP, a konfigurowanie i programowanie może być uproszczone, gdyż można zbudować system już z dwóch urządzeń firmy Stentofon. Aktualnie maksymalna pojemność systemu wynosi 16 urządzeń. W systemie można zastosować dowolne urządzenia SIP innych producentów. Pulse działa z wykorzystaniem istniejącej infrastruktury IP. Elementy podłącza się bezpośrednio do gniazda RJ45 sieci Ethernet, bez pośrednictwa jakichkolwiek bramek lub adapterów. Obsługa otwartych protokołów, w tym SIP, HTTP i XML, daje możliwość łatwej integracji i współpracy z innymi urządzeniami telekomunikacyjnymi, takimi jak centrale telefoniczne czy systemy bezpieczeństwa (CCTV lub KD).

Charakterystyka systemu

Konfiguracja systemu jest możliwa do przeprowadzenia za pomocą przeglądarki internetowej. STENTOFON Pulse jest wyposażony w prosty i intuicyjny interfejs, którego użycie znacznie skraca czas instalacji i uruchomienia. Podstawowa konfiguracja może trwać krócej niż dziesięć minut (czas zależy od liczby stacji zainstalowanych w systemie). Wszystko, co należy zrobić, to uruchomić oprogramowanie zarządzające i na wybranej stacji głównej wprowadzić nazwy pozostałych stacji. System nie zawiera centralnego serwera, dlatego wszystkie stacje interkomowe są po prostu podłączone do sieci LAN i to już wystarcza do prowadzenia rozmów.

Wszystkie stacje interkomowe STENTOFON IP mają wbudowany serwer SIP i serwer zarządzający. Jedna ze stacji

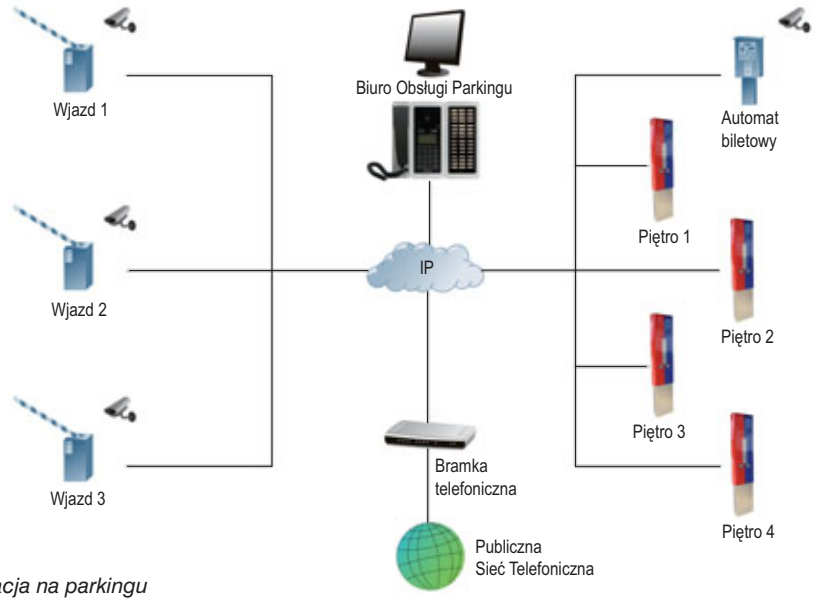
Rys. 1. Przykładowa minimalna konfiguracja

jest traktowana jako stacja główna i pełni rolę serwera SIP dla innych interkomów pracujących w tym systemie, a także dla telefonów i bramek IP. Nie ma centralnego serwera.

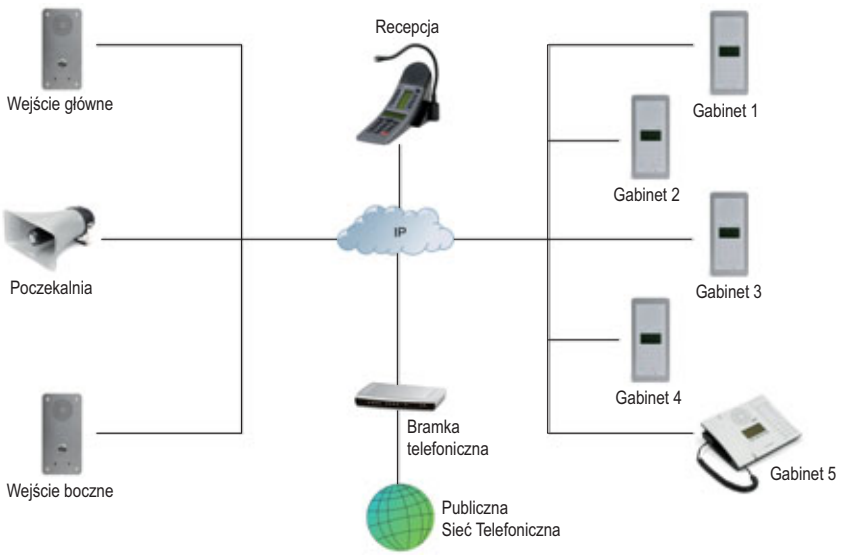
Interkomy sieciowe mają funkcję aktywnej redukcji hałasu oraz zapewniają transmisję dźwięku o jakości HD. Funkcja aktywnej redukcji hałasu jest zaimplementowana jako algorytm programowy w stacjach IP firmy STENTOFON. Wydajny procesor DSP znajdujący się w stacji analizuje sygnał pobierany z mikrofonu i wyznacza poziom hałasu w tym sygnale. Procesor DSP bardzo efektywnie usuwa sygnał hałasu, pozostawiając czysty sygnał mowy, nawet gdy poziom tego sygnału znajduje się znacznie poniżej poziomu otaczającego hałasu. Ta funkcja decydująco wpływa na poprawę zrozumiałości rozmowy prowadzonej w warunkach hałasu miejskiego, przez interkomy parkingowe czy interkomy służące do wzywania pomocy. Regulacja progu zadziałania tej funkcji jest możliwa w zakresie od 0 do 36 dB.

Aby osiągnąć jakość dźwięku HD, zaimplementowano szerokopasmowy kodek dźwięku G.722, który odwzorowuje ludzki głos w szerokim paśmie akustycznym, dzięki czemu mowa jest dużo bardziej naturalna i zrozumiała.

Protokół STENTOFON CCoIP (*Critical Communication over IP*) uwzględnia wszystkie potrzeby łączności w sytuacjach krytycznych. W tym celu wykorzystywany jest



Rys. 2. Przykładowa instalacja na parkingu



Rys. 3. Przykładowa instalacja w przychodni lekarskiej lub małym szpitalu

Rys. 4. Przykładowe urządzenia podłączane do systemu STENTOFON Pulse

protokół VoIP zapewniający przesyłanie dźwięku i danych. Mechanizmy zabezpieczające wbudowane w serwer AlphaCom XE zapewniają wysoki poziom bezpieczeństwa transmisji dźwięku i danych w sieci IP. Do głównych zabezpieczeń należą ograniczenia dostępu przy zarządzaniu systemem, oddzielny interfejs konfiguracyjny, wbudowany firewall, opcja V-LAN (IEEE 802.1Q) oraz kontrola dostępu do zasobów sieci (IEEE 802.1X).

Kompatybilność i skalowalność systemu Pulse nie stwarza ograniczeń dla użytkownika w przypadku, gdy ten zdecyduje o jego dalszej rozbudowie lub konieczności ściślejszej integracji z systemami bezpieczeństwa. Wszystkie stacje IP firmy STENTOFON mogą współpracować ze zintegrowanym serwerem interkomowym AlphaCom. Kolejną możliwością rozbudowy systemu Pulse jest możliwość instalacji stacji na dowolnym serwerze SIP takich producentów jak Cisco, Avaya AAstra, Asterisk.

Adam Gregorczyk
Novatel

SAMSUNG

LiteNet

Promocja kamer LiteNet HD

SSN Security Solution Network

Szczegóły w sieci dystrybucji **www.ssn.net.pl**

ALPOL SECURITY SYSTEMS

ProfiCCTV

NOVUS®

Profesjonalne rozwiązanie dla systemów zabezpieczeń

Nowe rejestratory cyfrowe z serii B

Ekonomiczna seria rejestratorów zaprojektowanych do ochrony średnich i małych obiektów

B seria

W serii B dostępne są rejestratory 4, 8 i 16 kanałowe z kompresją H.264 i prędkością zapisu do 400 kl/s w rozdzielczości D1. Najwyższe modele umożliwiają wyświetlanie na monitorze głównym obrazu w rozdzielczości Full HD na wyjściu HDMI. Rejestratory posiadają maksymalnie 3 wyjścia monitorowe, obsługują do 2 dysków wewnętrznych (łącznie do 4 TB) oraz są wyposażone w funkcję zapisu przedalarmowego do 30 sekund.

Podseria NDR-BA2000

NDR-BA2208
- 8 kanałów wideo
- 2 kanały audio
- **Nagrywanie „real-time" @ CIF**
- VGA, BNC
- 1 x SATA

NDR-BA2416
- 16 kanałów wideo
- 4 kanały audio
- **Nagrywanie „real-time" @ CIF**
- VGA, BNC
- 1x SATA

Podseria NDR-BA4000

NDR-BA4104
- 4 kanały wideo
- 2 kanały audio
- **Nagrywanie „real-time" @ D1**
- VGA, BNC
- 1x SATA

NDR-BA4208
- 8 kanałów wideo
- 4 kanały audio
- **Nagrywanie „real-time" @ D1**
- HDMI, VGA, BNC
- 2 x SATA

NDR-BA4416
- 16 kanałów wideo
- 4 kanały audio
- **Nagrywanie „real-time" @ D1**
- HDMI, VGA, BNC
- 2 x SATA

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

Nagrywanie 25 kl./s na każdym kanale w rozdzielczości D1

NDR-BA4104, NDR-BA4208, NDR-BA4416

D1 Real-Time RECORDING

Wyświetlanie Full HD na wyjściu HDMI

NDR-BA2416, NDR-BA4208, NDR-BA4416

Podgląd obrazu z kamer na telefonie komórkowym

iPhone Compatible · Windows Mobile Compatible · Android Compatible · BlackBerry Compatible · Symbian Compatible

Łatwe zarządzanie rejestratorami dzięki oprogramowaniu CMS

- Możliwość jednoczesnego połączenia z wieloma rejestratorami serii B
- Możliwość połączenia w trybie podglądu „na żywo" do 64 kamer
- Zdalna konfiguracja rejestratorów, odtwarzanie nagrań, kopiowanie nagrań
- Moduł zdalnego monitorowania zdarzeń systemowych (detekcja ruchu, aktywacja wejść alarmowych, utrata sygnału wideo)
- Dwukierunkowe połączenie audio
- Zdalna aktualizacja oprogramowania rejestratorów
- Wizualizacja obiektu (mapy)

CMS Compatible · Internet Explorer Compatible

Środki bezpieczeństwa fizycznego w ochronie informacji niejawnych (cz. 2)

Artur Bogusz
Marek Blim

W drugiej części cyklu autorzy, odnosząc się do dwu kolejnych etapów uproszczonego algorytmu przedstawionego w części pierwszej, chcą szerzej pokazać problemy związane zarówno z oceną istotności poszczególnych czynników składowych zasobu informacji niejawnych, jak i wpływem na nie różnorodnych (możliwych do zaistnienia) zagrożeń, w świetle stosowanych rozwiązań ochronnych (organizacyjnych, fizycznych technicznych) oraz przewidywanych postaci ryzyka

Wskazane w omawianym rozporządzeniu Rady Ministrów[1] zagrożenia naturalne i awarie[2] oraz wynikające z działań ludzkich – umyślnych lub przypadkowych – negatywne skutki[3] dla chronionego zasobu są ujęte wyłącznie w sposób sygnalny. Ustawodawca, wskazując określone grupy czynników (postać informacji i jej klauzula, ich ilość oraz dostępność), pozostawia tutaj „wolne pole dla decydenta/kierownika jednostki organizacyjnej (KJO wg uoin) funkcjonującego w danych warunkach (patrz: zał. 1 poz. 7 tabeli „Inne czynniki*)"), a rozszerzoną delegację daje w uzupełniającym zapisie na str. 10:

*) *Jeśli kierownik jednostki organizacyjnej uzna, że w jego jednostce występują inne niż wymienione w wierszach 1-6 tabeli czynniki mające wpływ na zagrożenie ujawnieniem lub utratą informacji niejawnych, powinien je określić, stanowisko uzasadnić (informacje zamieszcza się w rubryce "Uzasadnienie"), a następnie dokonać oceny istotności tych czynników. Ocenie podlegają wszystkie inne czynniki łącznie. Oznacza to, że jeśli w jednostce występuje tylko jeden z wymienionych czynników, należy go ocenić jako "bardzo istotny", "istotny" lub "mało istotny" dla zagrożenia ujawnieniem lub utratą informacji niejawnych. Jeśli w jednostce występują dwa lub więcej czynników z tej grupy, należy oszacować je łącznie i ocenić wpływ tych czynników na ocenę zagrożenia ujawnieniem lub utratą informacji niejawnych. W sytuacji gdy np. jeden z "innych" czynników został oceniony jako "bardzo istotny", a drugi jako "mało istotny", należy wskazać ocenę o najwyższym znaczeniu (w tym przypadku ocena istotności "Innych czynników" zostałaby wskazana na poziomie "bardzo istotnym"). W sytuacji gdy kierownik jednostki organizacyjnej uzna, że w jego jednostce czynniki wymienione w tabeli są nieistotne lub ich występowanie jest mało realne (np. zagrożenie ze strony obcych służb specjalnych) czynnik 7. powinien zostać oceniony jako "mało istotny".*

Jak wynika z powyższego, należy dość wnikliwie rozpatrzyć wszelkie spodziewane czynniki i możliwe do zaistnienia zagrożenia – ponosząc przy tym ryzyko niewłaściwego ocenienia ich istotności – decydujące o przyjętym do dalszych działań kwalifikowanym poziomie zagrożeń. Ponieważ ustawodawca pozostawia tę sprawę bez dalszych wyjaśnień, przyjrzyjmy się temu zagadnieniu nieco szerzej.

Określenie zagrożeń – czyli co wpływa na ryzyko ujawnienia lub utraty informacji

Analizując problem ujawnienia informacji objętych ochroną, czyli zakwalifikowanych jako ważne, trzeba wziąć pod uwagę zarówno znaczenie samych informacji dla ich właściciela i użytkownika, jak i potencjalne negatywne (dla niego i jego działań) konsekwencje rozszerzenia grona osób, które w wyniku ujawnienia nienależnie posiądą chronioną wiedzę.

Sama wiedza może podlegać ochronie z różnych względów, przykładowo z tytułu interesów:

- państwowych:
  - informacje niejawne własne (ogólne, resortowe, naukowe),
  - informacje niejawne powierzone (traktatowe, gospodarcze),
  - informacje niejawne udostępnione (układowe, sojusznicze),
- biznesowych:
  - informacje nieujawnione kontraktowe (zobowiązania zależne),
  - informacje nieujawnione organizacyjno-produkcyjne,
  - informacje nieujawnione techniczno-technologiczne,
- korporacji:
  - informacje nieujawnione dotyczące planów działania,
  - informacje nieujawnione dotyczące zarządzania kryzysowego,
  - informacje ukryte dotyczące stanu zasobów w sytuacjach nadzwyczajnych.

Zachowanie warunku konieczności ochrony tej wiedzy jest zależne od oceny stanu informacji, czyli od ich przydatności

1) *„Rozporządzenie RM z dnia 29 maja 2012r w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych" (Dz. U. z dn. 19 czerwca 2012 r., poz. 683).*

2) *Ibidem, § 3 ust. 5 pkt 1.*

3) *Ibidem, § 3 ust. 5 pkt 2.*

i znaczenia użytkowego. Takie podejście (w dotychczasowej praktyce) jest oczywiste; z zasady każdy z właścicieli lub dysponentów informacji jest w stanie zaakceptować fakt ich kwalifikowanego (pewnego) zniszczenia, ale raczej nie pogodzi się z ich potencjalnym przejęciem lub ujawnieniem osobom trzecim. Ryzyko tego typu zdarzenia jest zbyt duże dla dalszego poprawnego funkcjonowania instytucji (organizacji, firmy, korporacji)…

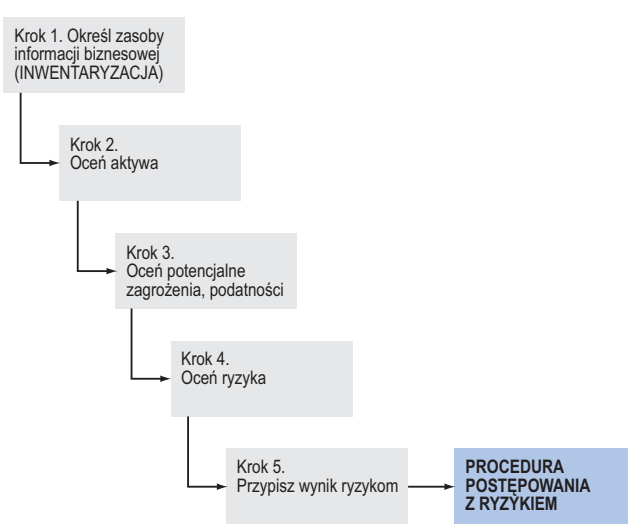
Przepisy o ochronie informacji niejawnych w ogóle nie dopuszczają kwestii ujawnienia tychże informacji w samej (obecnie dość szerokiej) definicji przetwarzania informacji niejawnych. Widać z nich jasno, że ustawodawca (czyli autorzy obowiązujących dziś przepisów) nawet podświadomie nie dopuszcza takiego postępowania z informacją niejawną jak jej ujawnienie. Dlaczego mielibyśmy nie brać tego pod uwagę? Skoro coś chronimy, skoro mamy określać, jak postępować, aby coś chronić, to musimy (przynajmniej powinniśmy) brać pod uwagę sposób postępowania, który ma doprowadzić do ujawnienia chronionej przez nas informacji. Inaczej algorytm naszego postępowania „ochronnego" będzie niepełny, będzie zakładał zbyt optymistycznie, że… to, przed czym się chronimy, nigdy nie wystąpi (!). Piszący te słowa mają wrażenie, że autorzy przepisów dotyczących ochrony informacji niejawnych nie zakładają w swoich rozważaniach możliwości ich ujawnienia.

A co, jeżeli wynika to tylko z braku wyobraźni co do zaistnienia takiej możliwości?

Postępowanie z ryzykiem w zakresie utraty lub ujawnienia informacji

Rozwiązania ochronne w obszarze ryzyk mają charakter głównie organizacyjny (tworzone są procedury oraz instrukcje) i stanowią podstawę do podjęcia działań materialnych (użycia środków fizycznej i technicznej ochrony). Tworzenie procedury postępowania z ryzykiem jest zawsze związane z inwentaryzacją i oceną posiadanych aktywów informacyjnych, przy czym należy podchodzić do ich podatności i wyceny od strony „negatywnego interesariusza" (czyli konkurenta biznesowego, intruza, agenta przemysłowego itp.), a nie od strony właściciela czy też legalnego dysponenta zasobu. Należy pamiętać, że dobrze opracowana procedura postępowania z ryzykiem nie tylko minimalizuje zagrożenie ujawnienia lub przechwycenia zasobu lub jego części, ale także w znaczącym stopniu ogranicza uzyskiwanie informacji o sposobie postępowania z posiadanymi chronionymi danymi.

Przykład tworzenia procedury na potrzeby ochrony informacji biznesowej obrazuje schemat postępowania przedstawiony na rys. nr 2.



Rys. 2. Algorytm budowy procedury postępowania z ryzykiem w biznesie (za: dr A. Wójcik, mat. e-Forum, Poznań 2011)

Postępowanie z ryzykiem w ochronie informacji niejawnych

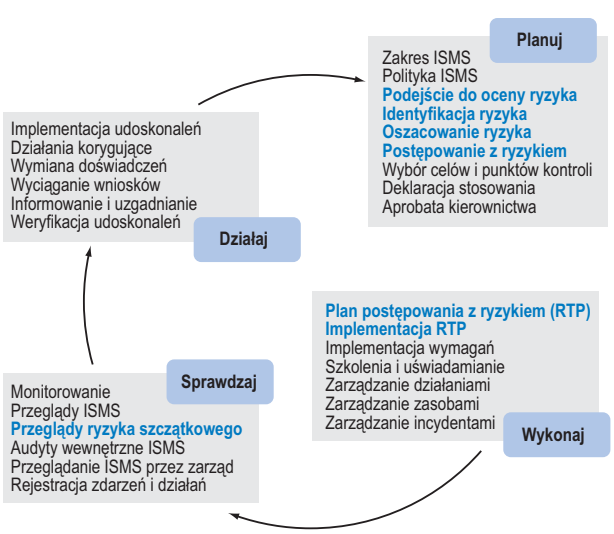
Bazując na posiadanym doświadczeniu zawodowym (jako rzeczoznawcy STZOiMoZB, audytorzy i kontrolerzy systemów bezpieczeństwa), autorzy usilnie rekomendują nie tylko korzystanie z obowiązujących zaleceń i wytycznych Służb (ABW[4]/SKW[5]) – oczywistych dla przypadków, gdy informacje posiadają klauzulę „poufne" lub wyższą – ale przede wszystkim zalecają zapoznawanie się z dobrymi praktykami wynikającymi z dobrowolnych norm oraz publikacji stowarzyszeniowych. Nie bez znaczenia dla pozytywnych skutków zastosowania jest zapoznanie się z udostępnionymi publicznie rozwiązaniami resortowymi (patrz: wytyczne Ministra Obrony Narodowej[6] czy decyzje Ministra Sprawiedliwości[7]) i przeniesienie do własnej praktyki ochronnej stosownych (rozsądnie przemyślanych)

4) www.abw.gov.pl; więcej: forum@abw.gov.pl.

5) www.skw.gov.pl; szczegóły: Zarząd Bezpieczeństwa Informacji Niejawnych zbin@skw.gov.pl.

6) Decyzja Nr 362/MON z dnia 28 września 2011 r. w sprawie wprowadzenia do użytku „Wytycznych Ministra Obrony Narodowej w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą »poufne« i »zastrzeżone«" (Dziennik Urzędowy Ministra Obrony Narodowej z 2011 r., Nr 20, poz. 302).

7) „Szczegółowy sposób organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych" (Dziennik Urzędowy Ministra Sprawiedliwości z 2011 r., Nr 2, poz. 14).



Analiza ryzyka: przykład niedoszacowanego elementu procesowego w realizowanych systemowo działaniach ochronnych obiektowych oraz informacyjnych.

Rys. 3. Postępowanie z ryzykiem w cyklu P-D-C-A dla SZBI/ISMS

elementów opisanych w nich rozwiązań organizacyjnych oraz technicznych.

Proponujemy odwołanie się do wieloletnich, sprawdzonych w praktyce działań opartych na doskonaleniu jakości zarządzania jako takiego, czyli do zastosowania we własnej ocenie naszego, analizowanego systemu bezpieczeństwa ryzyka – doświadczeń wynikających z cyklu Deminga (P-D-C-A, tzn. Planuj-Wykonaj-Sprawdzaj-Działaj) oraz traktowania systemowego wszystkich procesów w ramach SZBI/ISMS[8] (Systemu Zarządzania Bezpieczeństwem Informacji – Information Security Management System).

Zmiana przepisów w zakresie doboru środków bezpieczeństwa fizycznego (do której to zmiany odnoszą się nasze rozważania) wprowadziła kwestię postępowania z ryzykiem do jednego z podstawowych obowiązków osób odpowiedzialnych za ochronę informacji niejawnych. Dotychczas bowiem osoby odpowiedzialne za ochronę informacji sięgały do odpowiednich przepisów ustawy czy rozporządzenia, czytały je i wiedziały, jak zabezpieczyć informacje niejawne. O żadnym ryzyku nikt nie wspominał. Czy tego ryzyka nie było? Czy dotychczas nie zarządzano ryzykiem w ochronie informacji niejawnych?

Praktyka funkcjonowania zasad ochrony informacji niejawnych w uwarunkowaniach prawnych „starej ustawy" pokazuje, że tylko osoby, które dzięki swojemu doświadczeniu i umiejętnościom posiadały odpowiednie rozeznanie sprawy, korzystały z przedstawionego powyżej normatywnego procesu postępowania z ryzykiem, mimo że przepisy tego nie wymagały.

Postępowanie z ryzykiem w ochronie informacji biznesowych

Historia działań na rzecz biznesowego bezpieczeństwa informacyjnego – w tym analizy ryzyka i sposobu postępowania z nim w ramach ogólnie rozumianego zarządzania – rozpoczęła się na początku lat 90. XX wieku w Wielkiej Brytanii od prac biznesowych środowiska spółek handlowych i korporacji (w celu zmniejszenia strat i kosztów transakcji płatniczych z tytułu nieuprawnionego/fraudowego dostępu do kont). Doprowadziło to do powstania szeregu norm krajowych BS serii 7799[9]. Ich odzwierciedleniem użytkowym stały się normy i poradniki w krajach byłego dominium Korony Brytyjskiej (norma NS 27444 – Singapur, norma AS/NZS 4360 i HB 436 – Australia i Nowa Zelandia), a dowodem przydatności było przejęcie na szybkiej „ścieżce decyzyjnej" w ramach prac Komitetu ISO ustaleń krajowych UK i opublikowanie 15 grudnia 2000 r. normy międzynarodowej ISO 17799:2000. Norma ta była pierwszym niejako „kodeksowym" zapisem postępowania związanego z bezpieczeństwem informacji i jego zagrożeniami w świecie biznesu.

Stosowane w procesach biznesowych rozwiązania dotyczące zarządzania ryzykiem są ciągle doskonalone; alternatywą jest bowiem ponoszenie wysokich strat powstających w efekcie materializacji pominiętych lub zlekceważonych zagrożeń zamienionych w źle oszacowane (na ogół niedoszacowane) i nieprzewidywalne koszty bieżącej działalności firmy. Przykładem instytucji biznesowych wysokiego ryzyka są banki – ale one mogą służyć za wzorzec w zakresie form i metod analizy zagrożeń oraz sposobów postępowania z występującymi w nich różnorodnymi postaciami ryzyka[10].

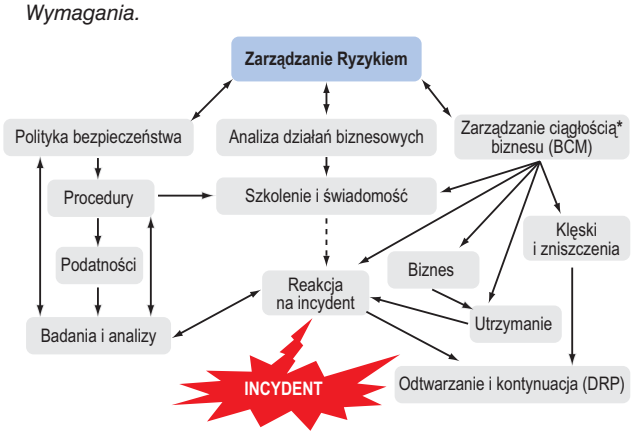
Kwestie związane z ryzykiem ujawnienia lub utraty informacji biznesowej występują w całym szeregu dokumentów dotyczących finansów, przedsiębiorczości, swobody działalności gospodarczej – wszędzie w połączeniu z egzekucją formalną (penalną, organizacyjną lub administracyjną) wobec zarówno osób winnych samych zaniedbań, jak i odpowiedzialnych z tytułu nadzoru nad prawidłowością postępowania (patrz: kodeksy: spółek handlowych, cywilny, karny; ustawy: o zwalczaniu nieuczciwej konkurencji, o ochronie baz danych, o dostępie do informacji publicznej, o prawie autorskim, prawo własności przemysłowej i in.).

Postępowanie z ryzykiem w biznesie jest tak oczywiste jak sam fakt, że biznes „nie wyjdzie", jeżeli nie weźmiemy pod uwagę określonych ryzyk. Dziś praktyka postępowania z ryzykiem w biznesie jest już tak mocno zautomatyzowana, że nikt się nad tym nie zastanawia. Po prostu wszyscy robimy, co trzeba. Każdy szanujący się zarząd podmiotu gospodarczego wie, że musi potrafić zarządzać odpowiednimi ryzykami dotyczącymi prowadzonego przez siebie biznesu.

Dla każdego biznesu informacja jest podstawą jego skuteczności w bieżącym funkcjonowaniu. Bez informacji – albo z informacją fałszywą lub taką, która przenika do firmy bez kontroli i nadzoru – trudno wyobrazić sobie prowadzenie efektywnego biznesu.

Jeżeliby biznes nie kierował się w swoim codziennym funkcjonowaniu kwestiami szacowania ryzyk związanych z ujawnieniem informacji biznesowych, to tego biznesu by po prostu nie było. Taką właśnie prostą metodę weryfikacji w tym zakresie pokazuje praktyka dnia codziennego.

8) *PN – ISO/IEC 27001:2007 Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*

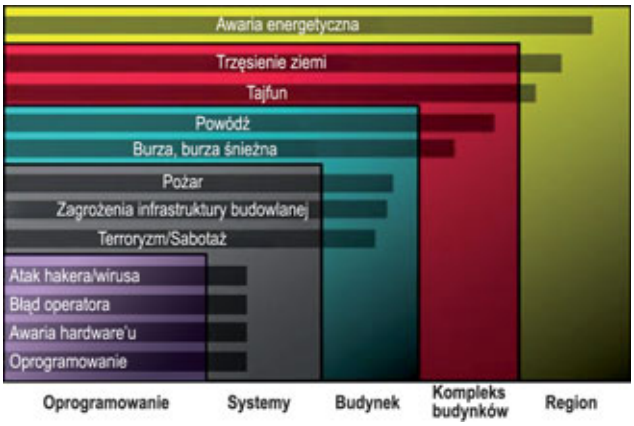


* Tytułem wyjaśnienia – akronim BCM jest w literaturze anglojęzycznej odczytywany dualnie, jako:
– Business Continuity Management (czyli ciągłość biznesowa – 1-3 lata);
– Business Constancy Management (czyli trwałość biznesowa – powyżej 5 lat).

Rys. 4. Zarządzanie ryzykiem w biznesie i jego interakcje

9) *Normy krajowe UK: BS 7799-1:1993; BS 7799-2:1996 i ich kolejne edycje (wspólna z 1998) oraz zmodyfikowane wydania (BS7799-2:2005; BS 7799-3:2006).*

10) *Międzynarodowe rekomendacje i ustalenia konferencji „Basel II", rekomendacje i zalecenia polskiego nadzoru bankowego (dawniej GINB, obecnie KNF).*



Rys. 5. Schemat rodzaju i obszaru występowania zagrożeń

Postępowanie z ryzykiem w ujęciu normatywnym

Z żalem należy stwierdzić, że ustawodawca, wskazując w przedmiotowym dokumencie dualność charakteru zagrożeń (§ 3 ust. 5 pkt 1 i 2) i pozostawiając KJO odpowiedzialność za ocenę istotności poziomu poszczególnych czynników (patrz: zał. 1 do rozporządzenia), nie odniósł się w dokumencie do istniejących w tym względzie dobrych praktyk z zakresu oceny ryzyka, zapisanych i dostępnych pod postacią norm (patrz: rys. 6), przewodników normatywnych[11] oraz zaleceń stowarzyszeniowych (np. materiały FERMA[12] i COSO[13]).

Strategiczny charakter zarządzania ryzykiem wynika nie tyle z samych zagrożeń, co z okoliczności ich powstania i ujawnienia się (procesy bieżące, działania kryzysowe oraz działania w sytuacjach nadzwyczajnych) pokazanych na schemacie (rys. 5).

Dla tak schematycznie przedstawionych obszarów opracowano cały szereg norm w różnych krajach, w Europie korzystamy głównie z brytyjskich (BS), które to doczekały się wersji międzynarodowych (ISO/IEC) oraz odniesień warunkowanych sytuacyjne (takich jak usługi I&CT czy zachowanie ciągłości działania), co prezentuje (po części) rys. 6.

Warto pamiętać, że elementy oceny ryzyka wynikające z przywołanych powyżej norm znalazły swoje odwzorowania w (nie do końca jawnych) zaleceniach wydanych przez ABW/SKW dla potrzeb bezpieczeństwa systemów informatycznych, a więc poniekąd… na wyższym poziomie wtajemniczenia. I tutaj pojawiają się pewne niejasności i nieścisłości. Powstała wprawdzie nowa ustawa, której jeden z rozdziałów traktuje o bezpieczeństwie informacji niejawnych w systemach teleinformatycznych; ponadto opublikowano stosowne rozporządzenie, które reguluje bardziej szczegółowe kwestie dotyczące bezpieczeństwa informacji niejawnych w systemach teleinformatycznych, ale w tym miejscu koniec jednolitości… gdyż wchodzimy na grunt *Zaleceń*, wydanych zarówno przez ABW, jak i przez SKW.

Obie instytucje nie stworzyły wspólnych opracowań w zakresie bezpieczeństwa informacji niejawnych w systemach teleinformatycznych. W wyniku tego stanu użytkownicy, administratorzy, inspektorzy i inne osoby, które z takich czy innych powodów mają do czynienia z niejawnymi systemami teleinformatycznymi, muszą tkwić w „dwuświecie" – ABW kontra SKW, SKW kontra ABW.

Taka sytuacja nie jest dobra i nie podnosi poziomu bezpieczeństwa informacji chronionych przetwarzanych we wspomnianych niejawnych systemach teleinformatycznych. Dotyczy to także elementów fizycznej ochrony tych systemów przedstawianych w *Zaleceniach*. Tymczasem dobre praktyki pokazują zagadnienie w sposób przystępny i użyteczny. Nie sposób orzec, dlaczego te ogólnie znane rozstrzygnięcia normatywne i stowarzyszeniowe nie zostały przywołane w załączniku nr 1 do omawianego rozporządzenia, zwłaszcza w świetle ścisłego odniesienia się do szeregu norm bezpieczeństwa technicznego (wyspecyfikowane w zał. nr 2 normy PN – EN), co uczyniło z dobrowolnych norm krajowych obligatoryjne wymagania normatywne, niezbędne do dalszej oceny stanu rzeczy w nakazanej do stosowania metodyce.

Atrybuty informacji a aspekty ochrony – czyli jakimi środkami dysponujemy

Rozpatrywany dokument jako podstawowe trzy atrybuty informacji przywołuje poufność, integralność oraz dostępność (patrz: § 2 pkt 1–3 rozporządzenia) z zagrażającym im incydentem bezpieczeństwa (patrz: § 2 pkt 4 rozporządzenia). Utrzymanie pożądanego stanu informacji jest celem zasadniczym (patrz: § 3 ust. 1), przy czym ustawodawca określa środki i sposoby oraz działania (patrz: § 4 ust. 1 i dalsze) służące do jego osiągnięcia.

Omawiane w tekście głównym rozporządzenia i w załącznikach środki bezpieczeństwa fizycznego stosuje się we wszystkich pomieszczeniach i obszarach, w których przetwarzane są informacje niejawne (IN). Przypomnijmy zatem, jakie czynności obejmuje przetwarzanie; są to:

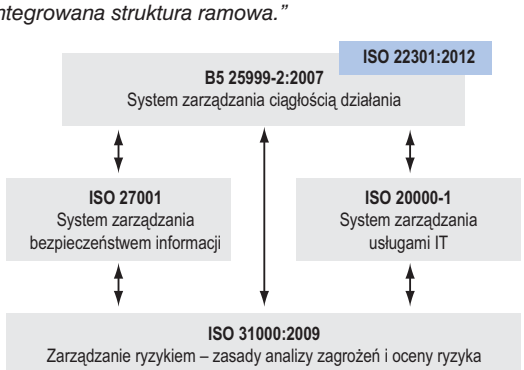
– zapoznanie z IN (niezależnie od postaci i nośnika),
– zapisanie IN (niezależnie od nośnika),
– modyfikacja IN (treści i postaci),
– przechowywanie IN (doraźne i archiwizacja),
– niszczenie IN (częściowa lub całkowita utylizacja informacji/nośników).

Ocena każdej z czynności dotyczy również miejsca, sposobu i systemu, w którym jest ona wykonywana (opis strefowania – patrz: § 5). Omawiany wcześniej wymagany nadzór nad bezpieczeństwem dla wymienionych czynności jest elementem podstawowym dla określenia parametrów i wytyczenia granic stref ochronnych zależnie od istniejących rozwiązań budowlanych (trwałości ścian i apretury otworów) oraz materiałów

11) *ISO Guide 73:2009 – „Zarządzanie ryzykiem – Słownictwo" (niestety nie istnieje tłumaczenie PKN).*

12) *FERMA – Federation of European Risk Management Associations – europejska wizja standardu zarządzania ryzykiem (www.ferma.eu/wp-content/uploads/2011/11/a-risk-management-standard-polish-version.pdf).*

13) *COSO 2004:2009 – „Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa."*



Rys. 6. Zależności norm w ocenie ryzyka

i urządzeń technicznych systemu bezpieczeństwa obiektu. Przykład ochrony budynku przedstawia rys. 7.

W praktyce oznacza to, że powinniśmy zbierać i analizować informacje z bliskiego otoczenia zewnętrznego obiektu które znajduje się poza naszym bezpośrednim zarządem i oddziaływaniem, ale przylega do granic naszej ochrony. Sama ochrona winna mieć charakter proaktywny[14]. Do dyspozycji mamy infrastrukturę budowlaną, sprzęt techniczny i system organizacyjny.

Rola ochronna infrastruktury budowlanej

Bezpieczeństwo fizyczne obiektu zależy w zasadzie od trwałości jego infrastruktury budowlanej, czasami wspomaganej dodatkowymi elementami strukturalnymi (takimi jak: wzmocnienia stropów – podciągi i wylewki samonośne; wzmocnienia ścian – panele lub zabudowa w pomieszczeniach konstrukcji kabin ekranujących). Zależy ono także od odporności mechanicznej zamontowanej w otworach apretury (drzwi, okien, wyciągów/czerpni itp.). Konstrukcja obiektu z jednej strony pozwala na montaż instalacji i systemów ochronnych, z drugiej zaś zapewnia dostatecznie dużą trwałość przegród mechanicznych, aby czas ich pokonania był dłuższy od czasu potrzebnego na dotarcie interweniujących sił ochrony fizycznej. W przedmiotowym rozporządzeniu zostało to ujęte w opisie kategorii K2: *Pomieszczenia*. Na początku charakterystyki tego środka bezpieczeństwa fizycznego zapisano, że o zaklasyfikowaniu pomieszczenia do danego typu decyduje najsłabszy element (tj. ściana, podłoga, strop, drzwi, okna). Rozporządzenie rozróżnia cztery typy pomieszczeń ze względu na konstrukcję budowlaną:

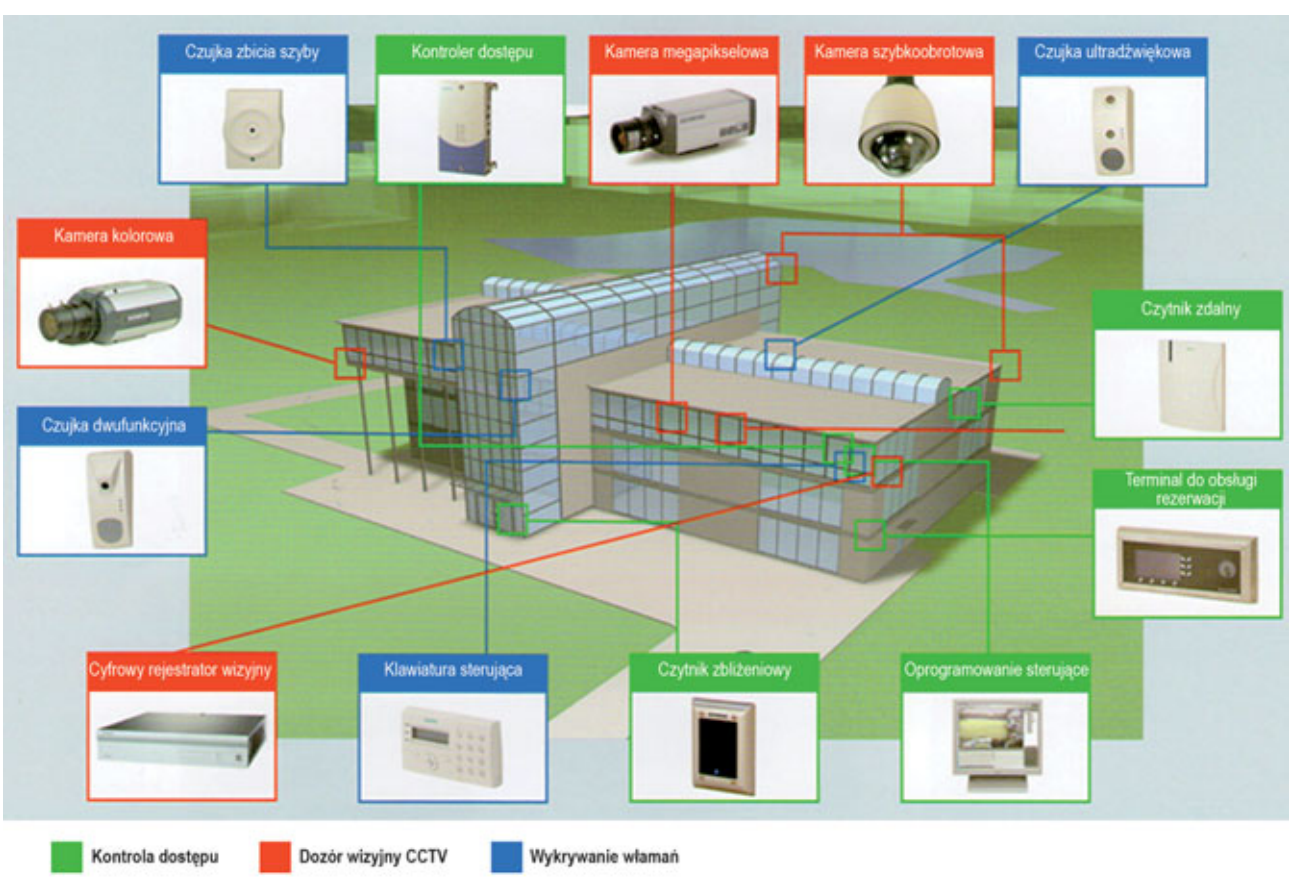
- pomieszczenie, którego ściany zostały zbudowane ze zbrojonego betonu o grubości 15 cm lub materiału o podobnej wytrzymałości,
- pomieszczenie, którego ściany zostały zbudowane z cegły lekkiej o grubości 25 cm lub materiału o podobnej wytrzymałości,
- pomieszczenie, którego ściany zostały zbudowane z cegły lekkiej o grubości 15 cm lub materiału o podobnej wytrzymałości albo ze sklejki oraz płyty gipsowej na ramie wspierającej,
- pomieszczenie, którego ściany zostały zbudowane z cegły lekkiej, gipsokartonu, drewna, płyt pilśniowych lub innego materiału o podobnej wytrzymałości.

Oczywiste jest, że odpowiednio winna być zachowana wytrzymałość oraz odporność podłóg i stropów w tych pomieszczeniach. Jeżeli chodzi o otwory (drzwi i okna), to rozporządzenie powołuje się na klasy wynikające odpowiednio z normy PN-EN 1627.

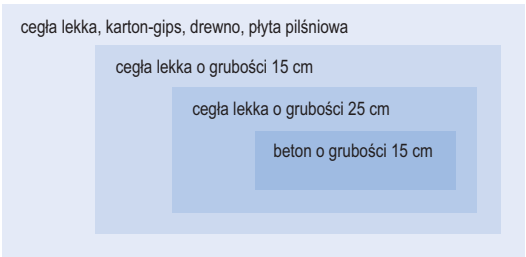
Rola ochronna infrastruktury alarmowej

Niezależnie od wszelkich dyskusji i obiegowych opinii na temat doskonałości systemów alarmowania i dozorowania

14) M. Blim, „Bezpieczeństwo obiektów. Poradnik techniczny", TECHOM, Warszawa 2012.



Rys. 7. Elementy ochrony obiektu – centrum konferencyjno-hotelowego (za: materiały z konferencji „Systemy zarządzania bezpieczeństwem informacji w jednostkach realizujących zadania publiczne", Warszawa 2011)



Rys. 8. Wymagania budowlane dotyczące pomieszczeń służących ochronie informacji niejawnych

technicznego[15], trzeba pamiętać, że dostępu bronią bariery mechaniczne i siły fizycznej ochrony, które to odpowiednio szybko ostrzeżone i powiadomione, są w stanie dotrzeć na miejsce incydentu oraz zatrzymać jego sprawcę.

Dodatkowym elementem jest tu dualność funkcjonowania infrastruktury alarmowej:

– W godzinach pracy zapewnia ona dostęp osób uprawnionych (SKD/RCP), ewentualnie przekazanie sygnałów alarmu napadowego ze wskazaniem jego lokalizacji, alarm i ewakuację doraźną (pożarową itp.) oraz nadzór wizyjny wybranych elementów obiektu (LCN – CCTV).
– Po godzinach pracy zapewnia ona trwałą ochronę oraz nadzór wizyjny wybranych elementów obiektu (LCN – SSWN/CCTV) z jednoczesnym dostępem patroli dyżurnych i interwencyjnych bezpośredniej ochrony fizycznej.

Nie wolno zapominać, że ta infrastruktura alarmowa wymaga zabudowanych trwale elementów antysabotażowych, współpracy operatorskiej w zakresie dozoru i przekazywania sygnałów o zaistniałych incydentach (w celu oceny stanu ochrony i prawdopodobieństwa fałszywego alarmu) oraz regularnych przeglądów i konserwacji (według norm obronnych minimum raz na kwartał). Ma to na celu wyeliminowanie możliwości zmanipulowania pracy urządzeń oraz oddziaływania na sprzęt różnych zmieniających się czynników (takich jak starzenie się czy zdarzenia eksploatacyjne).

Trzeba się również przyjrzeć, jak ustawodawca określa wymagania co do kontroli dostępu w kategorii K4. Jako podstawę doboru systemu kontroli dostępu podano w rozporządzeniu klasę rozpoznawania i klasę dostępu według wymagań określonych w normie PN-EN 50133-1, co oznacza, że najwyższy typ systemu kontroli dostępu powinien być wykonany w klasie rozpoznania 3 oraz klasie dostępu B. Natomiast najniższy typ systemu kontroli dostępu – przewidziany już tylko do zabezpieczania obszarów, w których przetwarzane są informacje niejawne o klauzuli co najwyżej „poufne" – powinien posiadać klasę rozpoznania 1 oraz klasę dostępu B. Wymagania są określone jednoznacznie i łatwe do sprawdzenia.

Trudniej jest o ocenę, gdy chodzi o wymagania dotyczące systemów sygnalizacji napadu i włamania. Zapisano bowiem, że system najwyższego typu musi spełniać wymagania określone w stopniu 4 określonym w normie PN-EN 50131-1; zapomniano natomiast o problemie lokalizacji systemu w terenie i jego rozległości oraz dostępności. Natomiast system najniższego typu musi spełniać wymagania dla stopnia 1 określonego w cytowanej normie – i jest to jedyne powiązanie, jakie można znaleźć w rozporządzeniu w kwestii odniesienia się do dotychczas obowiązujących klas systemów SA3 czy SA4. Jest to adnotacja, która mówi, że system spełniający wymagania klasy SA3 określone w PN-93/E-08390 można uznać za system najniższego typu określonego w rozporządzeniu, pod warunkiem spełnienia wymagań w zakresie ochrony i nadzoru (co jest nieco trudnym zadaniem ze względu na rozbieżności obu tych dokumentów).

Rola ochronna systemu organizacji bezpieczeństwa

Truizmem jest stwierdzenie, że najlepiej zaprojektowany system bezpieczeństwa jest martwy bez jego efektywnego wdrożenia, czyli zrozumienia oraz stosowania „tu i teraz" przez użytkowników – świadomych takiej potrzeby oraz znaczenia systemu dla codziennej praktyki bezpieczeństwa.

Ustawodawca w omawianym rozporządzeniu i jego załącznikach narzuca szereg czynności i wartości progowych ocen istniejącego stanu rzeczy, jak również zakłada przydatność i skuteczność użytych środków. Autorzy są świadomi, że u podstaw tego działania leży założony poziom wiedzy użytkowników na temat wymagań minimalnych i środków podstawowych stosowanych w systemach ochrony bezpieczeństwa informacji niejawnych, ale… czy jest to wiedza dostępna dla decydentów, czy też jedynie przekazana w ramach szkoleń ich pełnomocnikom ds. ochrony informacji niejawnych (OIN)? Praktyka pokazuje wyraźnie, że brak świadomości co do rzeczywistych zagrożeń oraz zapędy oszczędnościowe skutecznie paraliżują zamiary i niweczą nawet najlepsze plany pełnomocników ds. OIN, opracowane z myślą o doskonaleniu istniejących systemów.

Analizowane przez nas przedmiotowe rozporządzenie określa progowe wymagania dotyczące określonych środków bezpieczeństwa fizycznego, wskazując odpowiednie normy i inne przepisy prawa, zgodnie z którymi należy te wymagania określać. Nie precyzuje jednak, na podstawie jakich niezbędnych dokumentów organizatorzy ochrony informacji niejawnych w jednostce organizacyjnej mają dokonywać powyższej weryfikacji.

System sygnalizacji włamania i napadu, system kontroli dostępu, uwarunkowania stanu obiektu budowlanego czy inne środki powinny być wykonywane i odbierane w oparciu o stosowne dokumentacje techniczne, w skład których powinny wchodzić określone dokumenty niezbędne w procesie akredytacji pomieszczeń służących do przechowywania informacji niejawnych. Postawmy zatem istotne pytanie: „Jakie dokumenty powinien posiadać organizator systemu ochrony informacji niejawnych, aby wykazać w przypadku kontroli ABW/SKW, że w sposób właściwy dokonał doboru środków bezpieczeństwa fizycznego w pomieszczeniach stref ochronnych w swojej jednostce organizacyjnej?".

Niestety, próżno by szukać w rozporządzeniu odpowiedzi. Autorzy niniejszego artykułu, korzystając ze swojego dużego doświadczenia w zakresie funkcjonowania systemów ochrony informacji

15) Są to systemy współpracujące z LCN – lokalnym centrum nadzoru, SMA – stacją monitorowania alarmów, ewentualnie ACO – alarmową centralą odbiorczą, czyli odpowiednio: SKD – system kontroli dostępu (czasami połączony z RCP, czyli rejestracją czasu pracy), SSWN – system sygnalizacji włamania i napadu, CCTV – system zamkniętej pętli dozoru wizyjnego (Close Circle TV), zwanej czasami telewizją dozorową.

niejawnych, zdają sobie doskonale sprawę, że brak wskazania odpowiednich dokumentów z nazwy nie zwalnia organizatorów systemów ochrony informacji niejawnych w swoich jednostkach organizacyjnych od ich posiadania w sensie funkcjonalnym

Problem postrzegania ważności poszczególnych informacji (nie tylko tych *stricte* niejawnych, ale również ich dotyczących) przez przełożonych lub decydentów oraz użytkowników będzie omawiany w dalszej części cyklu.

Dostęp do informacji, nośników i systemów – kryteria strefowania

Przeglądając dotychczasowe dokumenty dotyczące fizycznej ochrony informacji, spotykaliśmy się z różnymi nazwami stref ograniczonego dostępu; były to odpowiednio:

- wg dokumentu RS-100 i procedur WEU/UZE[16] strefy:
  - *strefa złota* – w której możliwy był bezpośredni dostęp do dokumentów nawet o najwyższej klauzuli (np. FTS – Focal Top Secret; TSWEU – Top Secret WEU),
  - *strefa zielona* – w której przechowywane były dokumenty o różnej klauzuli, ale bez możliwości bezpośredniego zapoznania się z ich treścią po wejściu do strefy,
  - *strefa biała* – (poprzedzająca zieloną), w której przebywały osoby upoważnione, natomiast osoby z zewnątrz instytucji były nadzorowane lub eskortowane w drodze do personelu przyjmującego;
- wg dokumentu AD 70-1 i procedur NATO/OTP[17]:
  - *obszar bezpieczeństwa klasy I* – do którego wejście jest równoznaczne z dostępem do znajdujących się tam dokumentów i informacji niejawnych,
  - *obszar bezpieczeństwa klasy II* – w którym dokumenty są przechowywane w urządzeniach ochronnych i jest możliwy dostęp do nich,
  - *obszar bezpieczeństwa ogólnego/strefy administracyjne* – z kontrolowanym lub nadzorowanym dostępem osób i pojazdów, będący dla dwu poprzednich buforową strefą ochronną, pozwalającą na doraźny nadzór ze strony służb ochronnych,
  - *obszary bezpieczne technicznie (TSA)* – przeznaczone do niejawnych narad oraz prac kryptograficznych, wyposażone w klasyfikowane bezpieczne urządzenia oraz chronione technicznie (TSCM) przed wszelkimi przewidywalnymi formami podsłuchu akustycznego i elektronicznego;
- według „starej ustawy RP" i wydanej do niej rozporządzeń oraz wytycznych:
  - *I strefa* – do której wejście było równoznaczne z dostępem do znajdujących się w niej dokumentów i informacji niejawnych,
  - *II strefa* – w której w urządzeniach ochronnych były przechowywane dokumenty i był możliwy dostęp do nich na określonych odrębnie zasadach,

16) *WEU/UZE – Western European Union/Unia Zachodnioeuropejska, której RP była obserwatorem od 16 stycznia 1991 r., a członkiem od 25 kwietnia 1999 r., do momentu jej rozwiązania 31 grudnia 2005 r.*

17) *NATO/OTP – North-Atlantic Treaty Organization/Organizacja Traktatu Północnoatlantyckiego, której RP jest członkiem od 12 marca 1999 r.*

– *strefa administracyjna* – do której dostęp był nadzorowany, a osoby trzecie były odpowiednio traktowane (eskorta, pokój rozmów itp.).

Ustawodawca w § 5 rozporządzenia porządkuje te wszystkie dotychczas używane określenia i na nowo definiuje strefy fizycznej ochrony, łącząc i ujednolicając dotychczas używane opisy poszczególnych obszarów i pomieszczeń chronionych. Wydzielone zostały następujące strefy:

– *strefa ochronna I* – obejmująca pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji (§ 5 ust. 1 pkt 1),
– *strefa ochronna II* – obejmująca pomieszczenie lub obszar, w którym informacje niejawne o klauzuli „poufne" lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji (§ 5 ust. 1 pkt 2),
– *strefa ochronna III* – obejmująca pomieszczenie lub obszar wymagające wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów (§ 5 ust. 1 pkt 3),
– *specjalna strefa ochronna* – umiejscowiona w obrębie strefy ochronnej I lub strefy ochronnej II, chroniona przed podsłuchem, spełniająca dodatkowe wymagania bezpieczeństwa (§ 5 ust. 1 pkt 4).

Ponadto dopuszcza się utworzenie w strefie ochronnej I lub II pomieszczenia wzmocnionego, pozwalającego na przechowywanie informacji niejawnych poza szafami lub sejfami z bezpośrednim dostępem do nich.

Przedstawione kryteria strefowania i związane z nimi wymagania organizacyjno-techniczne jednoznacznie porządkują dotychczasowy „wieloukładowy nieład" pod względem opisu i nazw samych stref, ale dotyczy to informacji niejawnych o klauzuli „poufne" lub wyższej. Pozostawiono zatem w gestii KJO zakres metod oraz dobór środków dla informacji o klauzuli „zastrzeżone" (w poszczególnych resortach funkcjonują w tym względzie wyodrębnione rozwiązania).

Częstym błędem, jaki spotyka się przy próbie określenia stref w danej jednostce organizacyjnej, jest próba dopasowywania dotychczas obowiązujących definicji stref bezpieczeństwa i strefy administracyjnej do obowiązujących dziś definicji stref ochronnych. Przy tak przyjętej metodyce postępowania wniosek może być tylko jeden: tego nie da się zrobić, a nowe definicje są złe i nie pasują do niczego. Nie da się dopasować pojęć stref bezpieczeństwa i stref ochronnych.

Proces strefowania w jednostce organizacyjnej należy rozpocząć od dokładnego przeczytania i przyswojenia definicji zaproponowanych w rozporządzeniu. Następnie należy rozważyć potrzeby w zakresie konieczności przetwarzania informacji niejawnych określonych klauzul w poszczególnych obszarach danej jednostki organizacyjnej. Wtedy tak naprawdę proces strefowania będzie zakończony. Teraz tylko trzeba sprawdzić, czy w określonych uwarunkowaniach panujących w danej jednostce organizacyjnej wypełnia się wszelkie wymagania określone w poszczególnych definicjach.

Podsumowanie

Poprawność analizy własnej na rzecz wymaganej rozporządzeniem oceny istotności poziomów zagrożeń będzie bardzo trudna do uzyskania bez uzupełnienia wiedzy decydentów oraz ich personelu (w tym pełnomocników ds. OIN) o już funkcjonujące rozwiązania normatywne z zakresu analizy zagrożeń i oceny ryzyka.

W ocenie i rozważaniach dotyczących podejmowanych działań na pewno przydatna będzie specyfikacja techniczna ST 01 POLALARM, gromadząca w jednym opracowaniu kompendium wiedzy z zakresu systemów alarmowych, a jednocześnie odwołująca się do poszczególnych norm i rozwiązań praktycznych. W specyfikacji znajduje się szereg tabel z danymi do wyboru i zastosowania, ale są one poprzedzone wprowadzeniami użytkowymi, czego nie można powiedzieć o omawianym rozporządzeniu i jego załącznikach.

Artur Bogusz
Marek Blim

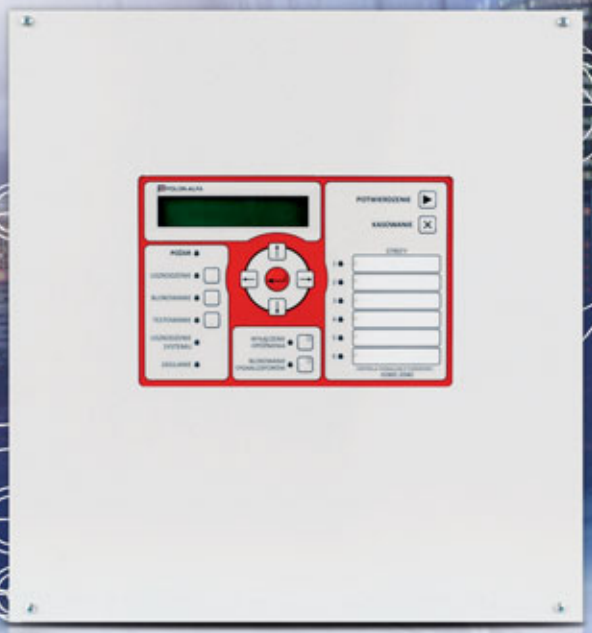
Bibliografia

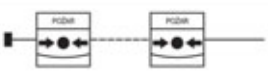
1. Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.
2. Blim M., *Bezpieczeństwo obiektów. Poradnik techniczny*, TECHOM, Warszawa 2012.
3. *Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych z załącznikami* (Dz. U. z dn. 19 czerwca 2012 r, poz. 683).
4. *Decyzja Nr 362/MON z dnia 28 września 2011 r. w sprawie wprowadzenia do użytku „Wytycznych Ministra Obrony Narodowej w sprawie określenia zasad postępowania z materiałami zawierającymi informacje niejawne oznaczone klauzulą »poufne« i »zastrzeżone«"* (Dziennik Urzędowy Ministra Obrony Narodowej z 2011 r., Nr 20, poz. 302).
5. ISO 17799:2005(2.ed.) ⇔ ISO/IEC 27002:2005 [PN-ISO/IEC 17799:2007] *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji.*
6. ISO Guide 73:2009 *Risk management - Vocabulary (Zarządzanie ryzykiem – Słownictwo*)
7. Krawiec J., Stefaniak A., *System zarządzania bezpieczeństwem informacji w praktyce. Zasady wyboru zabezpieczeń*, PKN, Warszawa 2012.
8. Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Konsalnet, Warszawa 2004.
9. NATO – AC/324-D(2002)1; The NATO Information Management, e-zin *www.nato.int*.
10. PN – ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.*
11. POLALARM ST 01/01. *Specyfikacja techniczna. Systemy alarmowe. Część 1: Systemy sygnalizacji włamania i napadu – Wymagania ogólne i zasady stosowania.*, Warszawa, 1 marca 2010 r.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

IGNIS 2040

OCHRONA PRZECIWPOŻAROWA MAŁYCH OBIEKTÓW



WEJŚCIA	IGNIS 2040	WYJŚCIA
 do 32 czujek punktowych		→ przekaźniki alarmu i uszkodzenia
 do 10 ręcznych ostrzegaczy pożarowych		→ zasilanie urządzeń zewnętrznych (24 V)
 czujka liniowa		→ linie sterujące sygnalizatorami
 czujki iskrobezpieczne	• od 4 do 6 linii dozorowych • 2 linie sterujące sygnalizatorami (zamiennie z liniami dozorowymi) • 5 lat gwarancji	→ odczyt pamięci zdarzeń

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

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

Ile różnych loginów i haseł musisz zapamiętać w pracy?

Krzysztof Białek

Obecnie trudno sobie wyobrazić życie bez komputera. Z większości programów czy stron internetowych można korzystać bez konieczności podawania dodatkowych, znanych tylko danemu użytkownikowi danych. Jeśli jednak program lub strona internetowa zawiera dane, które powinny być chronione, konieczne jest wprowadzenie dodatkowych zabezpieczeń

Najczęściej wymagane jest podanie nazwy lub numeru użytkownika (bardzo często bywa nim adres e-mail) oraz hasła. Banki stosują zazwyczaj dodatkowe zabezpieczenia, którymi są np. jednorazowe hasło wysłane na telefon komórkowy czy zmienne hasło wyświetlane na tokenie. Podobne zasady autoryzacji występują w programach użytkowych wykorzystywanych w firmach. Jeśli jest ich niewiele, użytkownicy nie mają problemu z zapamiętaniem loginów i haseł potrzebnych w różnych systemach. Problem pojawia się wówczas, gdy takich programów jest więcej. Najczęstszym błędem jest stosowanie przez użytkownika tych samych haseł w różnych systemach. Jest to o tyle niebezpieczne, że przechwycenie hasła do jednego systemu może umożliwić dostęp do innych. Jeszcze więcej problemów występuje wtedy, gdy system wymusza cykliczną zmianę hasła – np. raz w miesiącu. Zgodnie z założeniem taki mechanizm dodatkowo chroni system. Jeśli jednak użytkownik w swej codziennej pracy korzysta z wielu systemów wymagających odrębnej autoryzacji, zdarza się, że zapisuje sobie loginy i hasła w postaci jawnej, na przykład w notesie lub na karteczce przechowywanej w pobliżu komputera (w szufladzie biurka, pod klawiaturą) lub nawet przyklejonej do monitora, aby ich nie zapomnieć. Jest to rzeczywiście duże ułatwienie dla użytkownika, ale zarazem zagrożenie dla firmy. Niewielu użytkowników zdaje sobie sprawę z tego, iż będzie odpowiadać za skutki wykorzystania ich danych w systemie przez kogoś innego. Co zrobić, aby poprawić komfort pracy użytkowników systemów przy jednoczesnym zapewnieniu odpowiednio wysokiego poziomu bezpieczeństwa? W większych firmach, posiadających dużą liczbę stanowisk pracy, najczęściej wykorzystuje się autoryzację domenową, co oznacza, że użytkownik musi podać unikalną parę danych: login i hasło, aby móc korzystać z systemów służbowych, drukować dokumenty z wykorzystaniem drukarek sieciowych czy korzystać z Internetu. Coraz częściej programy użytkowe w firmach są aplikacjami webowymi (czyli, mówiąc w uproszczeniu, korzysta się z nich, używając przeglądarek internetowych) i w większości przypadków można w nich wykorzystać autoryzację domenową. Oznacza to, że użytkownik, który przy uruchomieniu systemu dokonał autoryzacji w domenie (podał login i hasło domenowe), jest po uruchomieniu programu użytkowego automatycznie autoryzowany w danej aplikacji – to system weryfikuje, czy użytkownik podał wcześniej login i hasło domenowe oraz czy jest uprawniony do dostępu do aplikacji. Aplikacja zostaje uruchomiona, jeśli dane są prawidłowe. Jeśli użytkownik nie posiada uprawnień, system poprosi o podanie innej pary danych autoryzacyjnych lub nie uruchomi się. Co jednak, jeśli w firmie nie stosuje się autoryzacji domenowej lub aplikacje użytkowe nie mogą zostać zintegrowane z domeną? Z pomocą przychodzi oprogramowanie typu SSO (*ang. Single Sign-On*) umożliwiające dostęp do wielu systemów po jednokrotnej autoryzacji. Jak to działa? Po pierwsze osoby odpowiedzialne za utrzymanie systemów informatycznych firmy muszą zainstalować tzw. agenta SSO, czyli odpowiednie oprogramowanie na konkretnych stacjach komputerowych, na których ma być możliwość jego wykorzystania. Następnie administrator (lub użytkownik posiadający takie umiejętności) musi określić, jakie systemy ma obsługiwać SSO i w jaki sposób automatycznie podawać dane autoryzacyjne w konkretnych aplikacjach. Gdy operacje te zostaną wykonane i SSO zostanie wdrożone, użytkownik, chcąc uruchomić aplikację wymagającą zalogowania, konfiguruje agenta, podając login i hasło dla każdej aplikacji z osobna (robi to tylko raz). Od tej chwili agent SSO przy uruchomieniu dowolnej aplikacji wymagającej autoryzacji zapyta tylko o jedno hasło. Po jego poprawnym wpisaniu będzie można uruchamiać różne aplikacje, a agent będzie podawać dane uwierzytelniające za użytkownika. Warto pamiętać, że odpowiednie skonfigurowanie SSO przez administratora może umożliwić również automatyczną, cykliczną zmianę hasła do danej aplikacji, jeśli jest ona wymagana. Od momentu skonfigurowania agenta SSO nie trzeba pamiętać loginu i hasła do konkretnej aplikacji, a jedynie jeden login i hasło do SSO.

Po przeczytaniu niniejszego artykułu czytelnikowi może nasunąć się pytanie: „Jak to możliwe, że SSO podnosi poziom bezpieczeństwa, skoro wystarczy przechwycenie loginu i hasła do SSO, by uzyskać dostęp do wielu aplikacji przeznaczonych dla konkretnego użytkownika?”. Otóż SSO stosuje się najczęściej z dodatkowym, zewnętrznym elementem uwierzytelniającym, który użytkownik musi posiadać. O ile login i hasło są wyłącznie danymi, zewnętrzny element uwierzytelniający jest fizycznym przedmiotem (najczęściej jest to karta z chipem, token podłączany do portu USB lub token wyświetlający zmienne hasła), który użytkownik musi posiadać przy sobie, więc osobie nieuprawnionej jest o wiele trudniej niepostrzeżenie wejść w jego posiadanie. Przy zastosowaniu takich zabezpieczeń uruchomienie systemu SSO – a jednocześnie jednokrotne logowanie i tym samym uzyskanie dostępu do wielu aplikacji – następuje po podłączeniu karty lub tokena do komputera i jednokrotnym podaniu hasła. Dzięki temu korzyść uzyskuje zarówno użytkownik (możliwość uzyskiwania dostępu do wielu różnych systemów po podaniu jednego hasła, bez konieczności zapamiętywania wielu różnych danych), jak i firma stosująca takie zabezpieczenia, ponieważ jednocześnie zabezpiecza się dostęp do aplikacji, a więc także do ważnych dla firmy danych.

Krzysztof Białek

Niemcy już wiedzą, jak lepiej dbać o dane

Paweł Markowski

Niemiecki Instytut Normalizacyjny opublikował normę DIN 66399, która na rynku niemieckim określa wymogi dotyczące urządzeń i procesów mających zagwarantować bezpieczne niszczenie danych znajdujących się na różnego rodzaju nośnikach. Nowa norma odnosi się nie tylko do dokumentów papierowych, ale również do mechanicznego niszczenia nośników optycznych, kart magnetycznych, pamięci flash, taśm magnetycznych i dysków twardych

Nowa niemiecka norma jest pierwszym tego typu rozwiązaniem na świecie. Poprzednia norma DIN 32757 odnosiła się wyłącznie do mechanicznego niszczenia dokumentów papierowych. Szybki postęp technologiczny sprawia, że z roku na rok coraz mniej informacji jest przenoszonych na papier. Obecnie nawet 90% informacji jest przechowywanych wyłącznie w formie elektronicznej. Nowa niemiecka norma jest zatem odpowiedzią na powszechną w firmach i instytucjach cyfryzację.

W Polsce, zgodnie z ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. Nr 133, poz. 883), wszystkie firmy oraz instytucje, które przechowują w swojej bazie dane osobowe, muszą chronić je przed wyciekiem. Korzystają one m.in. z firewalli, programów antywirusowych i haseł zabezpieczających. Nie można jednak zapominać o konieczności niszczenia elektronicznych nośników danych, które są wycofywane z użytku, w sposób uniemożliwiający odzyskanie tych danych.

Polskie prawo pozostawia firmom i instytucjom swobodę wyboru metody niszczenia nośników, ale zastrzega, że musi to być metoda gwarantująca skuteczność usunięcia zapisanych na nich informacji. Jest o tym mowa w VI punkcie rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji dotyczącej przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Większość aktualnie stosowanych metod, w tym wiórkowanie mechaniczne, nie uniemożliwia odczytania danych, a tylko mniej lub bardziej utrudnia lub podwyższa koszty ich odczytania, więc może nie spełnić powyższego wymogu. Ustawa o ochronie danych osobowych określa kary – nawet pozbawienia wolności – dla osób, które umożliwiły (choćby nieumyślnie) dostęp do danych osobowych, więc nieskuteczne usunięcie danych lub nieskuteczne zniszczenie nośnika danych może skutkować odpowiedzialnością karną.

Fot. 1. MCUD, czyli Mobilne Centrum Utylizacji Danych, to mobilne laboratorium najwyższej klasy

Nowa niemiecka norma DIN 66399 wyróżnia sześć kategorii nośników danych, które muszą być odpowiednio zniszczone w przypadku zaprzestania ich wykorzystywania. Oprócz nośników papierowych wymieniono płyty CD/DVD, dyski twarde, karty z taśmą magnetyczną, karty pamięci, karty chipowe. Nowa norma wprowadza też dwie dodatkowe klasy tajności – H-4 (dane „wysoce wrażliwe", klasa pośrednia między dotychczasowymi „poufnymi" i „tajnymi") oraz H-7 (dane „ściśle tajne"; konieczne jest dwukrotnie większe rozdrobnienie nośnika niż dotychczas na analogicznym poziomie). Łącznie norma mówi o siedmiu różnych poziomach tajności odnoszących się do dokumentów ogólnych, wewnętrznych, danych wrażliwych i osobistych, wysoce wrażliwych i osobistych, o fundamentalnej ważności dla instytucji oraz wymagających nadzwyczajnych zabezpieczeń ochronnych, a także ściśle tajnych. W zależności od statusu danych nośniki mają być mechanicznie rozdrabniane na wiórki o określonej wielkości.

O technologii LiquiDATA

Technologia LiquiDATA jest udostępniana w tzw. Mobilnym Centrum Utylizacji Danych (MCUD), czyli w specjalnie przystosowanym samochodzie-laboratorium. Klient może zamówić usługę i wskazać dowolny adres, pod którym zostanie wykonana (na terenie całego kraju). Dzięki temu wrażliwe dane mogą zostać zniszczone bez konieczności przewożenia ich na znaczne odległości i narażania na możliwość dostania się w niepowołane ręce. Technologia uzyskała pozytywną opinię ekspertów z Krajowego Stowarzyszenia Ochrony Informacji Niejawnych, Krajowego Stowarzyszenia Bezpieczeństwa Teleinformatycznego i Ochrony Informacji Niejawnych oraz Wojskowej Akademii Technicznej.

To niezmiernie ważne, że prawodawcy dostrzegają konieczność zmian w przepisach ze względu na rozwijającą się technologię. Coraz więcej danych przechowywanych jest w formie innej niż papierowa i muszą one zostać w pewnym momencie zniszczone. Niestety, nowa norma to nadal za mało, ponieważ odnosi się ona jedynie do mechanicznego

Fot. 2. We wnętrzu MCUD wykorzystano zaawansowane rozwiązania gwarantujące pełne bezpieczeństwo danych na talerzach dysków twardych, które poddawane są chemicznemu procesowi niszczenia

niszczenia nośników, pomijając na przykład chemiczne, i nie uwzględnia możliwości technologicznych w zakresie odzyskiwania danych z rozdrobnionych wiórków. Jest jednak niewątpliwie krokiem we właściwym kierunku.

Norma DIN 66399 powstawała przy współudziale firm produkujących niszczarki mechaniczne, dlatego odnosi się jedynie do mechanicznego rozdrabniania nośników i nie uwzględnia innych metod, nawet jeśli są one skuteczniejsze. Trzeba pamiętać, że można odzyskać dane nawet z najmniejszego fragmentu dysku twardego.

Najwyższa, 7. klasa tajności według normy DIN 66399 nakazuje, by nośnik został rozdrobniony na wiórki o wielkości nie przekraczającej 5 mm^2. O ile na skrawku papieru o takiej wielkości zmieści się zaledwie kilka liter, to fragment talerza dysku twardego o podobnych rozmiarach może mieścić nawet setki megabajtów danych. W przypadku danych szczególnie wrażliwych może to mieć niezwykle duże znaczenie dla ich właściciela – czy to z sektora prywatnego, czy publicznego. Jest to bardzo istotna wada tej normy, zwłaszcza, że od kilku lat nowoczesne laboratoria są w stanie odzyskać dane z powierzchni znacznie mniejszej niż 1 mm^2.

Choć w Polsce nie obowiązuje jeszcze krajowy odpowiednik niemieckiej normy, to warto przypomnieć, że liczne przepisy polskiego prawa nakazują skuteczne niszczenie danych. Przykładowo – zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 24 kwietnia 2004 r. nośniki informacji muszą być niszczone w sposób uniemożliwiający odczytanie zawartych na nich danych. Oznacza to, że wszelkie metody niszczenia nośników, które pozostawiają możliwość odzyskania danych, nie spełniają wymogów polskiego prawa.

Niemcy cenią porządek i ten porządek widać również w prawodawstwie i normach. Jego konsekwencją jest stworzenie nowej normy DIN 66399. Miejmy nadzieję, że również w Polsce odpowiednie instytucje dostrzegą potrzebę określenia standardów skutecznego usuwania danych i opracują stosowną normę, która uwzględni postęp technologiczny jeszcze bardziej niż norma niemiecka, jednak w tej chwili możemy jedynie powiedzieć, że to Niemcy mają normy, chociaż Polacy mają skuteczną technologię...

dr Paweł Markowski
BOSSG Data Security

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*

roger®

www.roger.pl

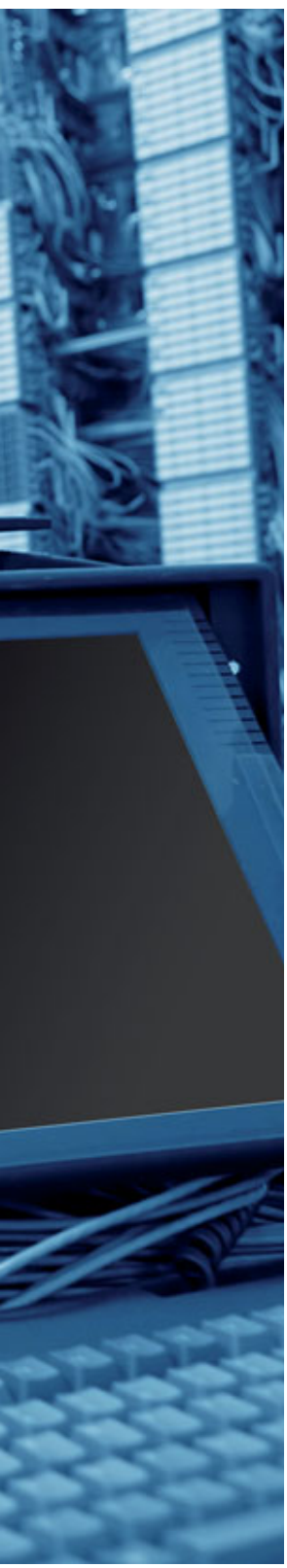
Rozwiązania Kontroli Dostępu i Rejestracji Czasu Pracy

Rozszerzono ofertę zaawansowanych kontrolerów dostępu o modele **PR612** oraz **PR622.** Urządzenia są zgodne funkcjonalnie z serią PRxx2, posiadają wbudowany czytnik kart EM 125 kHz i są przystosowane do pracy w warunkach zewnętrznych.

Bazy danych osobowych
kupię/sprzedam

Monika Brzozowska

W obecnych czasach przedsiębiorcom nie zawsze opłaca się samodzielnie tworzyć bazy danych osobowych. Często więc korzystają z dostępnych na rynku ofert sprzedaży baz danych osobowych. Oczywiście w tym miejscu trzeba zadać sobie pytanie, czy sprzedaż baz danych osobowych w ogóle jest legalna i dopuszczalna w Polsce. Wbrew pozorom odpowiedź na powyższe pytanie wcale nie jest jednoznaczna. Zależy bowiem czy osoby, których dane znajdują się w bazie, wyraziły zgodę na ich przetwarzanie, czy wyraziły zgodę na ich sprzedaż itp.



Ale zacznijmy od początku. Za dane osobowe uznaje się wszystkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (art. 6 ustawy o ochronie danych osobowych[1]). Dzięki sieci internetowej coraz częściej mówi się o nowej formie danych osobowych – tzw. danych cyfrowych. Choć nie jest to jednoznacznie określone, GIODO uważa za dane osobowe np. adresy e-mail. Wstrzymywałabym się jednak od uznania, że każdy adres e-mail jest daną osobową w rozumieniu ustawy. Im ogólniejszy adres, tym mniejsze prawdopodobieństwo uznania go za daną osobową. Przykładem może być *biuro@nazwafirmyXYZ.com*. Trudno wskazać tutaj tożsamość osoby kryjącej się pod danym adresem. Jeśli więc baza, którą zamierzamy kupić, będzie się składała z adresów e-mail, które to adresy nie będą – nawet w sposób pośredni – wskazywały na tożsamość osób, to nie możemy mówić w tym przypadku o bazie danych osobowych.

W większości jednak przypadków bazy danych zawierają zarówno dane techniczno-organizacyjne (np. adres firmy, telefon itp.), jak i dane kontaktowe osób fizycznych (np. rzecznika prasowego firmy, wymienionego z imienia i nazwiska, adres e-mail również składający się z imienia i nazwiska, telefon, miejsce urzędowania itp.). Wtedy faktycznie będziemy mogli powiedzieć, że w takiej bazie znajdują się dane osobowe.

Jakie są tego konsekwencje? Przede wszystkim administrator takiej bazy (podmiot, od którego chcemy ją zakupić) powinien spełniać co najmniej jedną z przesłanek, które umożliwiają przetwarzanie tego typu danych. Przesłanki te wymienione są w art. 23 ust. 1 ustawy o ochronie danych osobowych. Obalmy mity – nie zawsze na przetwarzanie danych osobowych potrzebna jest zgoda osoby, której dane są przetwarzane. Dane osobowe można przetwarzać również bez zgody osoby zainteresowanej, jeśli:

- jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- jest to konieczne do realizacji umowy – osoba, której dane dotyczą, jest jej stroną lub jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Zatem podmiot pragnący sprzedać dane powinien mieć albo zgodę każdej osoby zainteresowanej, albo wykazać, że przetwarzanie jest dopuszczalne jak w wymienionych wyżej przypadkach.

Załóżmy, że podmiot sprzedający bazę danych posiada zgody lub może się wykazać jedną ze wspomnianych przesłanek. Czy możemy zakupić taką bazę danych osobowych?

Samo nabycie baz danych osobowych nie jest nielegalne, warto jednak pamiętać o kilku aspektach towarzyszących tego działania.

Kupno bazy danych osobowych będzie traktowane jak przetwarzanie danych osobowych. W ustawie bowiem bardzo szeroko definiuje się pojęcie przetwarzania danych, zaś w orzeczeniach sądowych możemy znaleźć stwierdzenia: „nabycie w drodze umowy jest także sposobem uzyskiwania czy wydostawania (danych), co prowadzi do konkluzji, iż zakup bazy jest tożsamy z procesem ich zbierania i pozyskiwania”[2].

Uwaga! Nabycie bazy danych osobowych to nie to samo, co *outsourcing* usług (czyli np. przekazanie naszej bazy danych osobowych do biura rachunkowego, które rozlicza nas i naszych pracowników lub kontrahentów). Takie przekazywanie danych osobowych innemu podmiotowi, który ma dla nas wykonać usługę, bazując nich, jest nazywane w ustawie „powierzeniem przetwarzania danych”. Strony zawierają umowę, na podstawie której odbywa się właśnie owo przetwarzanie danych osobowych przez podmiot zewnętrzny. Nie jest to jednak sprzedaż bazy danych.

Wróćmy do obrotu bazami danych. Z punktu widzenia prawa najprostsza i najbardziej klarowna sytuacja jest taka, w której podmiot sprzedający dane osobowe posiada zgody zarówno na przetwarzanie tych danych, jak i na ich sprzedaż. Zgoda taka może przybrać postać oświadczenia woli, w którym osoba zainteresowana zgadza się na przetwarzanie i sprzedaż swoich danych osobowych innym podmiotom lub osobom trzecim. Jeśli owe podmioty nie będą wymienione z nazwy, przyjmuje się, że zgoda na sprzedaż danych osobowych jest uzależniona od tego, czy dane te będą przetwarzane w takim samym celu, w jakim zostały zebrane.

Możliwe jest również oświadczenie zawierające w swojej treści nazwy podmiotów, którym dane mogą być (lub będą) przekazane. Wówczas przekazanie danych podmiotom innym niż wskazane w oświadczeniu będzie oznaczało wyjście poza uzyskaną zgodę osoby zainteresowanej (tj. osoby, której dane zostały zebrane).

W przypadku posiadania zgody na sprzedaż danych osobowych nie ma konieczności, by podmiot sprzedający bazę takich danych zwracał się do osób zainteresowanych o ponowne wyrażenie zgody. Nawet mimo znacznego upływu czasu od udzielenia takiej zgody nie ma potrzeby, by uzyskiwać ją ponownie. Zgoda może być bowiem w każdym czasie odwołana.

1) Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. Nr 133, poz. 883.

2) Wyrok NSA z 13 lipca 2004 r., OSK 507/04, CBOSA.

Warto w tym miejscu wskazać, że nabywca bazy danych osobowych powinien wypełnić pewne obowiązki informacyjne. Zgodnie z art. 25 ust. 1 ustawy w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą (czyli np. w przypadku zakupu bazy danych osobowych), administrator danych jest zobowiązany poinformować tę osobę, bezpośrednio po utrwaleniu zebranych danych, o:

1) adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku;
2) celu i zakresie zbierania danych, a w szczególności o odbiorcach lub kategoriach odbiorców danych;
3) źródle danych;
4) prawie wglądu do swoich danych oraz ich poprawiania;
5) prawie żądania zaprzestania przetwarzania danych osobowych z uwagi na szczególną sytuację lub prawie wniesienia sprzeciwu.

Problematyczna natomiast może okazać się sytuacja, gdy podmiot sprzedający bazy danych nie posiada zgody na sprzedaż. Czy więc taka sprzedaż będzie legalna? Kwestia ta nie została jednoznacznie rozstrzygnięta w doktrynie.

Wyobraźmy sobie, że firma X zbiera dane osobowe w celach marketingowych. Zbieranie takich danych w celu marketingu bezpośredniego własnych produktów lub usług jest legalne na podstawie art. 23 ust. 1 pkt 5 ustawy. Ale czy legalna jest dalsza sprzedaż tych danych osobowych?

Zdaniem niektórych ekspertów przepis art. 26 ustawy o ochronie danych osobowych uniemożliwia sprzedaż bazy danych bez zgody osób, których dane dotyczą. Zgodnie z tym przepisem administrator danych przetwarzający je powinien ze szczególną starannością ochronić interesy osób, których dane dotyczą. W szczególności jest zobowiązany zapewnić, aby dane te były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Dlatego można uznać, że z tej zasady należy wyprowadzić zakaz przetwarzania tych danych dla tego samego celu, lecz przez innego administratora[3].

Wydaje się jednak, że możliwa jest też inna argumentacja, tj. uznanie, że dozwolona jest sprzedaż bazy danych osobowych bez zgody osób, których dane dotyczą, a jedynie z późniejszym poinformowaniem tych osób o sprzedaży ich danych osobowych (co stanowi zrealizowanie obowiązku informacyjnego wskazanego w art. 25 ust. 1 ustawy o ochronie danych osobowych).

Wyobraźmy sobie, że nasza firma X zbiera dane osobowe w celu marketingu bezpośredniego. Na mocy ustawy o ochronie danych osobowych firma X, jako administrator, powinna poinformować osobę zainteresowaną o swoim adresie, celu i zakresie przetwarzania danych osobowych itd. Administrator danych osobowych informuje o tym osobę, której dane osobowe są przetwarzane, i w tej sytuacji osoba ta ma prawo do:

1) pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację (art. 32 ust. 1 pkt 7);
2) wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach wymienionych w art. 23 ust. 1 pkt 4 i 5 ustawy, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych (art. 32 ust. 1 pkt 8).

Wydaje się więc, że wobec brzmienia art. 32 ust. 1 pkt 8 ustawy administrator danych (firma X) może przekazać bazę danych osobowych innemu administratorowi (firmie Y), jeśli zostaną spełnione następujące warunki:

1) osoba zainteresowana otrzyma wszystkie informacje wskazane w art. 25 ust. 1 ustawy o ochronie danych osobowych;
2) osoba zainteresowana nie wniesie sprzeciwu wobec przekazywania danych;
3) nie zostanie zmieniony cel przetwarzania danych osobowych.

Trzeba podkreślić, że zdaniem GIODO firma marketingowa, która kupiła bazę danych od innego podmiotu, powinna powiadomić każdą osobę o tym, że przetwarza jej dane[4]. GIODO uznał również, że do sprzedaży danych osobowych konieczna jest wyraźna zgoda osoby zainteresowanej[5].

Podsumowanie

Kwestie związane z kupnem i sprzedażą baz danych nie są jednoznacznie uregulowane. Nabycie baz danych (w tym baz danych osobowych) nie jest w Polsce zabronione i w obrocie gospodarczym występuje coraz częściej.

Nierozstrzygniętą kwestią jest możliwość sprzedaży bazy danych osobowych (i nabycia jej) w sytuacji, gdy zbywca (ani siłą rzeczy nabywca) nie posiada zgody osoby zainteresowanej na przetwarzanie jej danych osobowych. Wydaje się jednak, że przy spełnieniu odnośnych przesłanek – jak zbieranie danych zgodnie z prawem (przesłanka legalizacyjna), poinformowanie osób zainteresowanych o adresie, celach, odbiorcach danych itp., a także przetwarzanie ich w tym samym celu co zbywca – zbywca nie będzie musiał mieć zgody osoby zainteresowanej na sprzedaż jej danych osobowych. Pogląd ten może jednak wydać się kontrowersyjny.

Najkorzystniejszą – z punktu widzenia prawa – sytuacją jest posiadanie zgody nie tylko na przetwarzanie danych osobowych, ale również na ich sprzedaż.

Monika Brzozowska (adwokat)

Autorka jest partnerem w kancelarii PDB LEGAL Pasieka, Derlikowski, Brzozowska i Partnerzy, specjalistą w dziedzinie ochrony dóbr osobistych i danych osobowych, praw autorskich oraz prawnych aspektów funkcjonowania cyberprzestrzeni. Jest także ekspertem Instytutu Sobieskiego.

3) J. Barta, P. Fajgielski, R. Markiewicz, "Ochrona danych osobowych. Komentarz", LEX nr 106662.

4) Odpowiedź na pytanie „Czy firma marketingowa, która kupiła bazę danych osobowych od innego podmiotu, powinna powiadomić każdą osobę o tym, że przetwarza jej dane?", http://www.giodo.gov.pl/318/id_art/3355/j/pl/ [online].

5) Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2007, s. 45.

Ty i Twoi klienci możecie spać bezpieczniej

z systemem PowerMaxExpress!

Wysoce stabilny i **niezawodny**
bezprzewodowy system alarmowy

Oszczędzasz czas i **pieniądze**
dzięki szybkiej i bezproblemowej instalacji!

Visonic
A Tyco International Company

Wyłączny dystrybutor produktów Visonic 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

Depozytor na klucze systemowe SAIK LOCK

SAIK LOCK

Depozytor SAIK LOCK służy do bezpiecznego przechowywania, wydawania i przyjmowania kluczy. Każdy klucz znajdujący się w szafce jest chroniony i dostęp do niego mają tylko uprawnione osoby.

Klucze deponowane są w sposób uniemożliwiający podgląd ich profilów w trakcie przechowywania. W szafkach typu SAIK LOCK istnieje możliwość zastosowania systemów klucza generalnego dowolnego producenta. Jeśli funkcjonują one już w przedsiębiorstwie, nie ma potrzeby wymiany kluczy.

Wszystkie zdarzenia zachodzące w systemie są przez niego rejestrowane z uwzględnieniem daty, czasu oraz danych użytkownika i umożliwiają tworzenie szczegółowych raportów w oparciu o przyjęte kryteria.

Szafka SAIK LOCK wyposażona jest w duży ciekłokrystaliczny wyświetlacz z panelem dotykowym. Umożliwia to wygodne korzystanie z dodatkowych funkcji systemu - na przykład wbudowanej Rejestracji Czasu Pracy – czy wyświetlanie komunikatów od administratora.

Najważniejsze cechy

- Pobranie klucza tylko przez osoby upoważnione
- Zwrot klucza do dedykowanego otworu chroniącego profil klucza
- Wielkość depozytora dowolnie dostosowana do potrzeb klienta
- Duży, kolorowy wyświetlacz LCD z panelem dotykowym
- Standardowo montowany czytnik kart Mifare lub Unique
- Możliwość współpracy z dowolnym innym czytnikiem kart
- Możliwość współpracy z różnymi systemami kontroli dostępu, alarmowymi lub ppoż.
- Wbudowane akumulatorowe zasilanie awaryjne
- Dołączone oprogramowanie instalowane na dowolnej liczbie komputerów pozwalające na pełną kontrolę nad obiegiem kluczy w firmie
- Możliwość podglądu stanu szafki z poziomu przeglądarki internetowej
- Możliwość wyboru dowolnego koloru z palety RAL
- Możliwość dowolnej rozbudowy systemu
- Współpracuje z depozytorami wyposażonymi w tzw. breloki (typu SAIK KEY)
- Możliwość wbudowania kamery nadzorującej osoby korzystające z depozytora
- Podłączenie szafek do sieci LAN
- Wbudowana rejestracja czasu pracy (RCP)
- Możliwość dostosowania depozytora do potrzeb klienta

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

SAIK SOFT – elektroniczny system wsparcia portiera

System SAIK SOFT to rozwiązanie dla tych firm i instytucji, które potrzebują łatwo i kompleksowo usprawnić organizację obiegu kluczy używanych przez pracowników.

Osoby odpowiedzialne za wydawanie kluczy wyposażone są w elektroniczny Rejestrator Portiera SAIK SOFT. Za pomocą tego urządzenia każde wydanie i zwrot klucza jest odnotowywane przez dołączone oprogramowanie. Dzięki niemu zawsze istnieje możliwość kontroli nad tym kto, kiedy i jaki klucz pobrał.

Co równie istotne, pracownicy mogą dostać tylko ten klucz, do którego mają uprawnienia i tylko w godzinach określonych przez administratora. Takie rozwiązanie pozwala skrócić do niezbędnego minimum czas potrzebny na pobranie i zwrot klucza, zachowując jednocześnie obowiązujące standardy bezpieczeństwa.

System SAIK SOFT posiada także wbudowany moduł rejestracji czasu pracy (RCP), dzięki temu każde przyłożenie przez pracownika karty do czytnika może określać jego czas pracy. W ten sposób system SAIK SOFT można wykorzystywać dla wszystkich pracowników, lub tylko dla wydzielonej ich części.

Zastosowanie SAIK SOFT całkowicie eliminuje konieczność wypełniania i przechowywania dokumentów takich jak np. księga ewidencji kluczy, książka wejść-wyjść, zeszyt wyjść służbowych. Dzięki temu przewyższa te rozwiązania funkcjonalnością i ilością gromadzonych informacji.

Zaawansowane oprogramowanie, składające się z części administracyjnej, raportowej i alarmowej pozwala na dostosowanie systemu do indywidualnych potrzeb Klienta. Typ rejestratora, liczba obsługiwanych kluczy oraz inne elementy systemu mogą być dowolnie dopasowane do wymagań obiorcy.

Najważniejsze cechy

- Identyfikacja użytkowników w oparciu o osobiste karty zbliżeniowe
- Do każdego klucza przypięty jest brelok, na którym zaszyfrowane są informacje umożliwiające identyfikację klucza
- Każdy pracownik posiada przypisane do siebie klucze
- Elastycznie definiowane przedziały czasowe dostępu do kluczy
- Akumulatorowe zasilanie awaryjne Rejestratora Portiera
- Łatwa wymiana kluczy, możliwa do wykonania przez administratora
- Archiwizacja wszystkich zdarzeń zachodzących w systemie
- Wielostanowiskowe oprogramowanie systemowe pozwalające na przyjazne administrowanie systemem
- Gwarancja jakości i prawidłowej pracy systemu – produkt polski
- Stała 24 h obsługa techniczna
- Wbudowana rejestracja czasu pracy (RCP)

Producent:

bt electronics

bt electronics sp. z o.o.
Kraków, ul. Dukatów 10
31-431 Kraków

tel. 12 429 36 16, faks 12 410 85 11
e-mail: kontakt@saik.pl
www.saik.pl, www.bte.pl

Kamera BFF-41F

Kamera BFF-41F jest następcą znanej i cenionej kamery BBB-31F. Cechą wyróżniająca jest zastosowanie procesora Effio-P, czyli najbardziej zaawansowanego procesora DSP w rodzinie procesorów Effio firmy Sony. Najważniejszą cechą kamery jest WDR, czyli poszerzony zakres dynamiki, który poprawia zdolność do obserwacji scen o dużym zróżnicowaniu jasności.

W odróżnieniu od uproszczonych sposobów realizacji funkcji WDR wykorzystywanych w tańszych kamerach, w BBB-31F do realizacji tej funkcji stosowany jest przetwornik Sony Double Scan z podwójnym skanowaniem. W wyniku połączenia procesora DSP Efio-P oraz przetwornika Double Scan powstała kamera o wysokiej czułości i bardzo wysokiej rozdzielczości (700 TVL), wyróżniająca się bardzo dobrym odwzorowaniem kolorów i świetną dynamiką.

Kamera przeznaczona jest do zastosowań wymagających precyzyjnej regulacji parametrów, takich funkcji jak 3D DNR czy BLC/WDR/Eclipsa i przede wszystkim do obserwacji scen z jasnymi źródłami światła, np. drzwi wejściowych do budynku czy terenu zewnętrznego z silnymi punktowymi źródłami światła.W przypadku wykorzystania podświetlenia w podczerwieni należy pamiętać by zastosować obiektyw z korekcją w IR, gdyż w przeciwnym razie obraz będzie rozmyty.

Zalety

- Przetwornik Double Scan
- Poszerzona dynamika kamery WDR
- Cyfrowa stabilizacja DIS
- Redukcja szumów 3D DNR, która w porównaniu ze standardową redukcją DNR zapewnia zmniejszenie smużeń przemieszczających się obiektów
- Funkcja DSS x512, zwiększająca czułość kamery podczas pracy w trybie nocym, odsuwany mechanicznie filtr podczerwieni
- Możliwość pracy w dzień i w nocy
- Możliwość współpracy z reflektorami emitującymi promieniowanie podczerwone
- BLC – czyli kompensacja tylnego oświetlenia
- Sterowanie przez port RS485 – protokół Pelco-D

Właściwości

- Bardzo wysoka rozdzielczość 700 TVL
- Przełączanie w tryb BW przy niskim poziomie oświetlenia
- Czułość 0,1 lx (kolor), 0,0003 lx (kolor, DSS wł.), 0,01 lx (B/W) 0,000007 lx (B/W, DSS wł.)
- OSD, regulacje jasności oraz koloru, AGC, WDR, Eclipsa, BLC, AWB, 3D DNR, DIS, Flickerless, D/N, DZ – regulacja przez OSD
- Detekcja ruchu, strefy prywatności, funkcja mirror w pionie i poziomie oraz obrót obrazu, wyostrzanie obrazu, sterowanie przez RS485 (Pelco-D)
- Zasilanie 12 V_{DC}

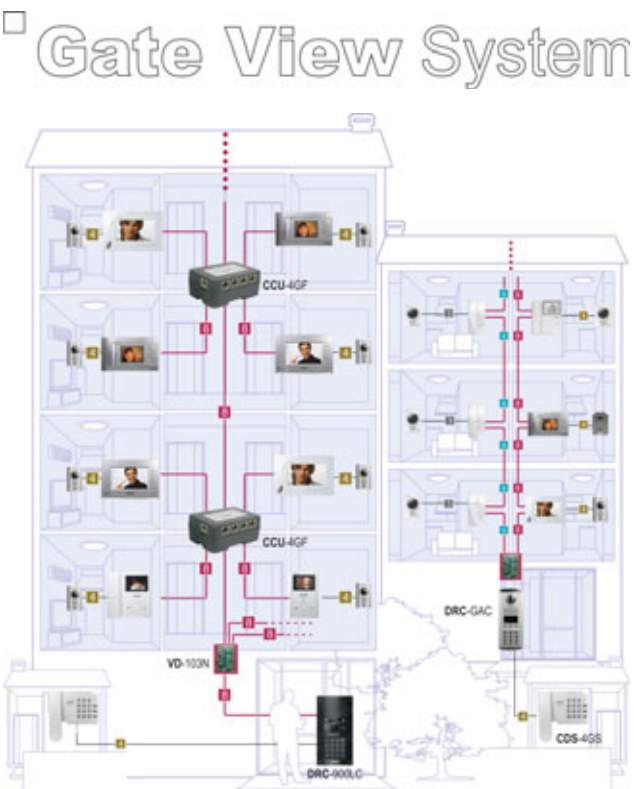
Dystrybucja: GDE POLSKA

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

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.

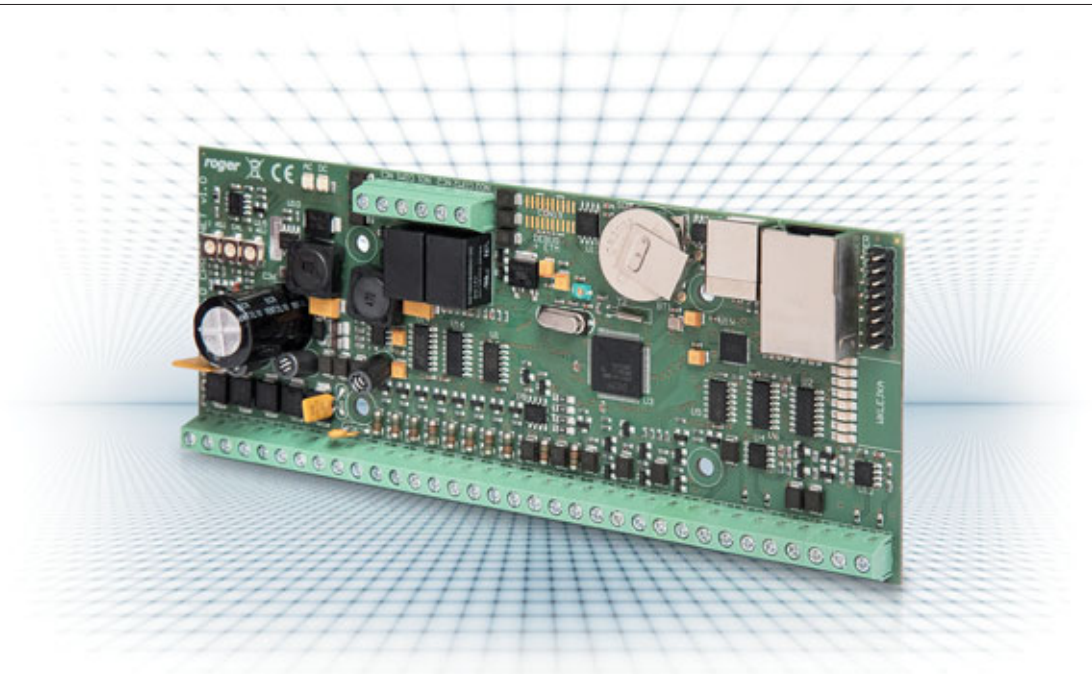
Dzięki połączeniu funkcjonalności monitorów analogowych z urządzeniami cyfrowymi system może być w prosty sposób rozbudowany przez dodanie indywidualnych paneli wejściowych lub dodatkowych kamer obserwacyjnych. Jeżeli na terenie obiektu znajduje się pomieszczenie ochrony, może ono być również wyposażone 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

Centrala CPR32-NET
Centrala systemu kontroli dostępu RACS 4 z interfejsem IP/Ethernet



Centrala CPR32-NET stanowi kolejną, rozwojową wersję oferowanej od kilku lat centrali kontroli dostępu typu CPR32-SE. Ten nowy produkt realizuje wszystkie funkcje swojego poprzednika, a dodatkowo oferuje szereg nowych możliwości, z których najważniejsze to możliwość programowej integracji z centralami alarmowymi INTEGRA (wymagany jest interfejs INT-RS) oraz możliwość współpracy z zamkami mechatronicznymi serii SALLIS (firmy SALTO). Zrealizowana w centrali CPR32-NET koncepcja integracji z centralami INTEGRA polega na możliwości sterowania uzbrojeniem stref alarmowych, zarówno z poziomu manipulatorów systemu alarmowego jak i czytników systemu kontroli dostępu. Ponadto system kontroli dostępu pobiera i wyświetla w swoim logu zdarzeń pewne krytyczne zdarzenia pochodzące z systemu alarmowego w wyniku czego operator systemu może się ograniczyć do monitorowania jednego wspólnego logu zdarzeń. Nowa centrala oferuje także opcję zapisu zdarzeń na wymiennej karcie pamięci FLASH co powoduje, że zastosowanie odpowiednio dużej karty pamięci może w praktyce zabezpieczyć bufor zdarzeń na kilka lat pracy systemu bez zagrożenia jego przepełnieniem. Komunikacja z nową centralą odbywa się przez sieć LAN/WAN z wykorzystaniem standardu szyfrowania AES 128.

Charakterystyka

- Obsługa systemu złożonego z maks. 32 kontrolerów serii PR
- Osiem wejść parametrycznych
- Sześć wyjść tranzystorowych 15 V_{DC}/1 A
- Dwa wyjścia przekaźnikowe 30 V/1,5 A
- Zarządzanie harmonogramami czasowymi i kalendarzami
- Wbudowany interfejs komunikacyjny IP/Ethernet
- Szybka, szyfrowana transmisja danych pomiędzy centralą a komputerem zarządzającym
- Wbudowany nieulotny bufor pamięci o pojemności 250 tys. zdarzeń z możliwością rozszerzenia o dodatkową kartę pamięci
- Realizacja funkcji globalnych (Strefy Alarmowe, Globalny Antipassback itd.)
- Integracja programowa z centralami alarmowymi Integra (firmy SATEL)
- Integracja programowa z zamkami mechatronicznymi Sallis (firmy SALTO)
- Zasilanie 18 V_{AC} lub 12 V_{DC}
- Wbudowany zasilacz impulsowy z wyjściem 12 V_{DC}/1 A
- Aktualizacja oprogramowania wbudowanego (firmware)

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

PR612/PR622
Nowe kontrolery dostępu serii zaawansowanej

Kontrolery PR612 oraz **PR622** firmy Roger są następcami popularnego kontrolera PR302. Oba urządzenia posiadają wbudowany czytnik standardu EM 125 kHz, zegar czasu rzeczywistego oraz bufor pamięci do rejestracji zdarzeń występujących w systemie kontroli dostępu. Kontrolery PR612 i PR622 mogą być stosowane jako autonomiczne punkty kontroli dostępu lub tworzyć sieć w ramach systemu kontroli dostępu RACS 4 obejmującego różne kontrolery pojedynczego przejścia.

Charakterystyka

- Jedno- lub dwustronna kontrola drzwi
- Możliwość dołączenia czytnika serii PRT (Roger) w celu obustronnej kontroli przejścia
- Obsługa do 4000 użytkowników
- Bufor pamięci na 32000 zdarzeń
- Zasilanie 12 V_{DC}
- Trzy wejścia NO/NC
- Dwa wyjścia tranzystorowe 15 V_{DC}/1 A
- Wyjście przekaźnikowe 30 V/1,5 A
- Wbudowana klawiatura numeryczna (tylko PR612)
- Wbudowany głośnik
- Ochrona antysabotażowa (tamper)
- Komunikacja przez RS485 z zastosowaniem dowolnej topologii magistrali komunikacyjnej
- Funkcje typu wejście komisyjne, wejście warunkowe, losowa kontrola użytkowników i inne
- Integracja z systemami alarmowymi, systemami rejestracji czasu pracy oraz telewizją dozorową
- Tryby drzwi: normalny, zablokowane, odblokowane i warunkowo odblokowane
- Tryby identyfikacji: karta lub PIN, karta i PIN, tylko karta, tylko PIN
- Kontrola dostępu w windach (wymagany moduł XM-8)
- Praca w warunkach zewnętrznych

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

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

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 Borkiewicz 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. 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. 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

ASSA ABLOY

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, 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
faks 52 387 54 66 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

EUROPEAN SECURITY TRADING POLSKA Sp. z o.o.
Al. Jerozolimskie 133 lok. 13
02-304 Warszawa
tel./faks 22 115 71 50
e-mail: kontakt@estpolska.pl
www.estpolska.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
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 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 49 79
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./faks 17 857 80 60
e-mail: sawel@sawel.com.pl
www.sawel.com.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

SCHRACK SECONET POLSKA Sp. z o.o.
ul. Domaniewska 44a
02-672 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
Jacek Giersz
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

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. 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

SECURITY SOLUTION NETWORK Sp. z o.o.
ul. Obornicka 276
60-693 Poznań
tel. 61 842 29 62
faks 61 842 29 62
e-mail: ssn@ssn.net.pl
www.ssn.net.pl

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

Biuro Handlowe:
ul. Rzymowskiego 30, 02-697 **Warszawa**
tel. 22 843 83 95
faks 22 843 79 12
e-mail: tap5@tap.com.pl

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 97
faks 42 611 12 98
e-mail: zbar@zbar.com.pl
www.zbar.com.pl

Nazwa firmy	produkcja	projektowanie	dystrybucja	instalacja	szkolenia
AAT Holding	–	TAK	TAK	–	TAK
ACSS ID Systems	–	–	TAK	–	TAK
AGIS Fire & Security	–	TAK	TAK	TAK	TAK
Alarm System	TAK	TAK	TAK	TAK	–
Alarmnet	–	–	TAK	–	–
Alarmtech Polska	TAK	TAK	TAK	–	–
Alkam System	TAK	TAK	–	TAK	–
Alpol	–	–	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	–	TAK
CMA	TAK	–	–	TAK	–
D-MAX	–	–	TAK	–	–
DG Elpro	–	TAK	TAK	TAK	–
Dyskam-Ekotrade	TAK	TAK	–	TAK	–
Dyskret	–	TAK	TAK	TAK	–
EBS	TAK	TAK	TAK	–	–
Ela-compil	TAK	–	TAK	–	–
El-Mont	TAK	–	–	TAK	–
Elproma	–	TAK	–	TAK	–
Eureka	–	TAK	–	TAK	–
EST POLSKA	–	–	TAK	–	TAK
Factor Polska	–	TAK	TAK	–	TAK
FES	–	TAK	TAK	TAK	TAK
GDE Polska	–	–	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	–	–
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	TAK	–	–	TAK
Sawel	–	TAK	TAK	TAK	TAK
Schneider Electric Buildings Polska	TAK	–	TAK	–	–
Schrack Seconet Polska	TAK	TAK	TAK	–	TAK
Secural	TAK	TAK	TAK	–	TAK
SMA	–	TAK	–	TAK	–
SPS Electronics	–	TAK	TAK	–	TAK
SSN	–	–	TAK	–	–
Tap – Systemy Alarmowe	–	–	TAK	–	TAK
Technokabel	TAK	–	–	–	–
UNICARD	TAK	TAK	TAK	TAK	TAK
W2	TAK	TAK	TAK	–	–
Vision Polska	–	–	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	–	–
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
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
bt electronics	–	–	TAK	–	–	TAK	–	TAK	–
CAMSAT	–	TAK	–	–	–	–	TAK	–	–
CBC (Poland)	–	TAK	–	–	–	–	–	–	–
CMA	TAK	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	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	–	–
EST POLSKA	TAK	TAK	TAK	–	TAK	–	TAK	–	–
Factor Polska	TAK	TAK	TAK	TAK	TAK	–	–	TAK	TAK
FES	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	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	–	–
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	–	–	TAK
Schneider Electric Buildings Polska	TAK	TAK	TAK	–	–	TAK	–	–	–
Schrack Seconet Polska	–	–	–	TAK	–	–	–	–	–
Secural	TAK	TAK	TAK	TAK	TAK	TAK	–	TAK	TAK
SMA	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SPS Electronics	TAK	TAK	TAK	TAK	–	–	TAK	–	–
SSN	–	TAK	TAK	–	–	–	–	–	–
Tap – Systemy Alarmowe	TAK	TAK	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	–	–	–	–	–
ZBAR	TAK	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

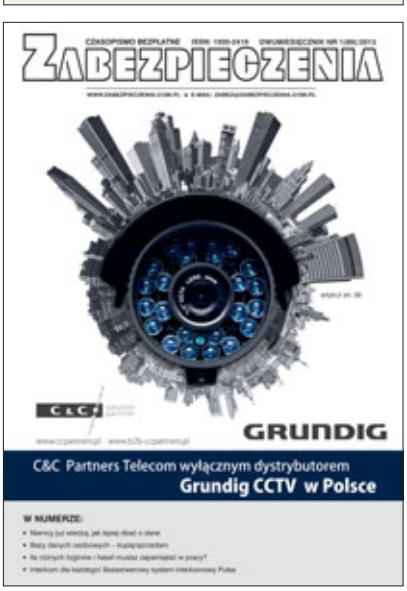
Współpraca
Marcin Buczaj
Adam Bułaciński
Piotr Czernoch
Marcin Pyclik
Sławomir Wagner
Andrzej Wójcik

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

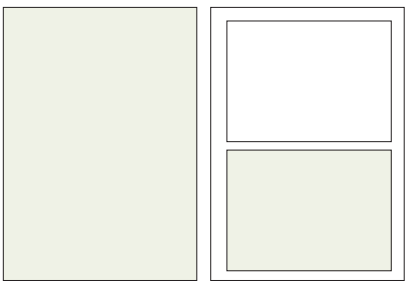
Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka



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)

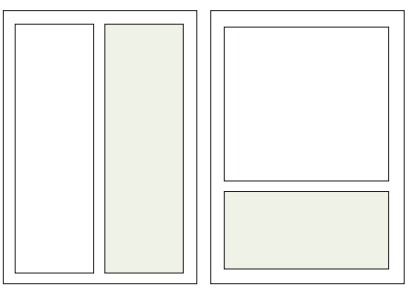
1/2 strony (170 x 125 mm)

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)

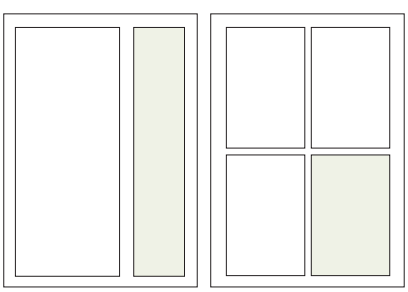
1/3 strony (170 x 80 mm)

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

AAT Holding	47, 56, 77
ACSS ID Systems	46
ADI	19
Axis Communications	43
Bosch Security Systems	34
C&C Partners Telecom	1
Euroalarm	72
GDE Polska	26
Gunnebo	27
HID	2
HSK Data	23
Jablotron Alarms	51
MJ Training	18
Optex Security	65
Polon-Alfa	67
Roger	73
SALTO Systems	96
Samsung Techwin Europe	31
Satel	95
Security Solution Network	55
ZBAR	35

Systemy alarmowe **Satel**

Niezawodna komunikacja

GSM-5
NOWOŚĆ

Zadaniem modułu komunikacyjnego GSM-5 jest zapewnienie dodatkowych torów łączności GSM/GPRS uzupełniających komunikację wykorzystującą tradycyjną linię telefoniczną.

Obsługa dwóch kart SIM pozwala podnieść niezawodność łączności GSM dzięki uniezależnieniu się od infrastruktury jednego operatora telekomunikacyjnego.

Moduł GSM-5 pozwala realizować powiadamianie głosowe oraz SMS, jak również prowadzić monitoring z wykorzystaniem technologii GPRS i CSD. Niewątpliwym atutem urządzenia jest możliwość zdalnej konfiguracji oraz aktualizacji oprogramowania z użyciem GPRS.

Więcej informacji na:
www.satel.pl

Satel

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

Poznaj zalety i możliwości
systemu SALTO

SALTO
inspiredaccess

NOWY POZIOM KONTROLI DOSTĘPU

- innowacyjność
- wirtualna sieć SVN
- kontrola dostępu w czasie rzeczywistym
- bezprzewodowa technologia Wireless
- wysokie standardy bezpieczeństwa
- brak problemów z kluczami
- możliwość rozbudowy istniejacych systemów
- niskie koszty instalacji
- prosty montaż

bezprzewodowe okucia

elektroniczne wkładki

sieciowe czytniki
naścienne

inteligentne zamki
do szafek

SVN data-on-card inside. SALTO inspiredaccess

IP66 SALTO GDO INGRESS PROTECTION

Protected by BioCote Antibacterial Technology

SKG®

SALTO wireless real-time access control

SALTO
inspiredaccess

SALTO Systems sp. z o.o.
Oddział w Polsce
ul. OSTROBRAMSKA 101A
04-041 WARSZAWA

kontakt@saltosystems.com
www.saltosystems.pl