CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 6(130)/2019

ZABEZPIECZENIA

RACS 5

Skalowalny system kontroli dostępu, bezpieczeństwa i automatyki

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

Identyfikacja mobilna

roger®

Intelligence for Building

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A.

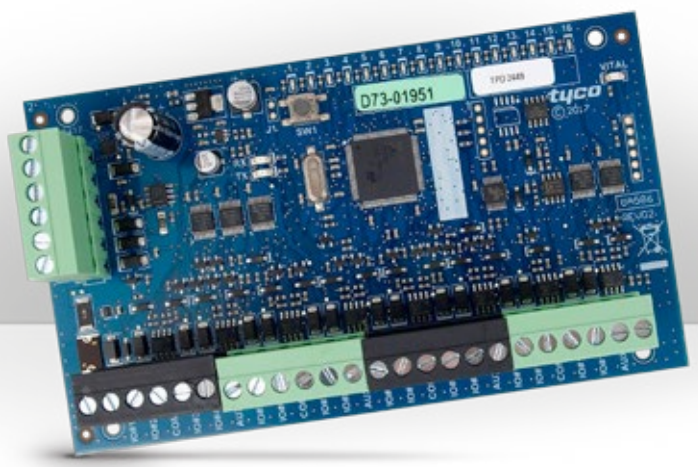
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

SPIS TREŚCI

Nowości produktowe

Wydarzenia, informacje

Nowy moduł rozszerzeń we/wy KT-MOD-IO16 do kontrolerów firmy Kantech



Firma **Kantech** wprowadziła do swojej oferty nowy moduł rozszerzeń przeznaczony do współpracy z kontrolerami **KT-1** i **KT-400**. Moduł zawiera szesnaście wyprowadzeń zakończonych zaciskami, które mogą pracować jako linie dozorowe lub jako wyjścia sterujące. Wyprowadzenia, które są skonfigurowane jako linie dozorowe, mogą być parametryzowane z użyciem jednego lub dwóch rezystorów. Wszystkie wyprowadzenia są podzielone na cztery jednakowe grupy, a każda z nich może mieć niezależnie skonfigurowany tryb pracy, dlatego jest to bardzo elastyczne i ekonomiczne rozwiązanie, które użytkownik może łatwo dostosować do swoich potrzeb. Do każdego z wyżej wymienionych kontrolerów można podłączyć wiele takich modułów rozszerzeń, poprzez port COM2 (RS485 – szyfrowane w standardzie AES 128), i otrzymać 256 wejść i 256 wyjść. Ostatni moduł na magistrali RS485 może być oddalony o 1200 m od kontrolera. Moduły są zasilane z wyjścia AUX kontrolera lub oddzielnego zasilacza 12 V_{DC} w zależności od liczby modułów i obciążenia wyjść sterujących.

Szczegółowe parametry i sposób okablowania są podane w instrukcji montażu modułu.

Kontrolery mogą współpracować z modułami tego typu pod warunkiem, że mają fabryczne oprogramowanie układowe w wersji 2.xx lub wyższej, zaś oprogramowanie systemowe EntraPass jest w wersji 8.10 lub wyższej. Zaciski śrubowe umożliwiają łatwe dołączenie przewodów. Szesnaście wskaźników LED sygnalizuje stan wyjść sterujących, co znacznie ułatwia diagnostykę. Typowe zastosowanie to podłączenie czujek alarmowych lub sterowanie pracą windy z wykorzystaniem czytnika kart zbliżeniowych zainstalowanego w kabinie windowej. Na uwagę zasługuje fakt współpracy takich modułów z kontrolerem KT-1, który do tej pory miał tylko cztery wyprowadzenia we/wy i nie mógł być wykorzystany do współpracy z windami.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING
Opracowanie: Redakcja

TP-Link T1500-28PCT

wydajny przełącznik PoE do systemów nadzoru wizyjnego

Przełącznik **Smart T1500-28PCT** jest urządzeniem zaprojektowanym z myślą o ekonomicznych systemach monitoringu IP, dostosowanym do potrzeb małych i średnich firm. Do najważniejszych zalet urządzenia należą prosta instalacja i zarządzanie oraz niskie koszty instalacji.

Przełącznik T1500-28PCT ma 24 porty PoE zgodne ze standardami IEEE 802.3at/802.3af, o sumarycznej mocy 192 W. Urządzenie współpracuje z bezprzewodowymi punktami dostępowymi, kamerami i telefonami IP oraz innymi urządzeniami dostosowanymi do zasilania metodą PoE. Pozwala to wyeliminować niepotrzebne okablowanie i tym samym obniżyć koszty instalacji.

Przełącznik został wyposażony w cztery porty RJ45 10/100/1000 Mb/s i dwa gigabitowe gniazda combo SFP.

Aby zapewnić lepszy przekaz dźwięku, danych i lepszą transmisję strumieni wizyjnych w sieci, urządzenie korzysta z zaawansowanych opcji QoS. Administratorzy sieci mogą określić priorytety w ruchu sieciowym, np. dla poszczególnych adresów IP, adresów MAC, portów TCP lub UDP. Dzięki temu nie ma opóźnień w transmisji dźwięku i obrazu. W połączeniu z obsługą sieci VLAN sprawia to, że transmisje głosowe są płynne i wydajne.

Przełącznik T1500-28PCT jest urządzeniem łatwym w obsłudze i zarządzaniu. Ma intuicyjny graficzny interfejs użytkownika obsługiwany poprzez przeglądarkę internetową. Obsługa protokołów SNMP w wersji 1, 2 lub 3 oraz RMON umożliwia urządzeniu wysyłanie komunikatów o nieprzewidzianych zdarzeniach oraz monitorowanie jego stanu przez użytkownika.

Bezpośr. inf. Iwo Ostalski
TP-Link Polska

Ochrona i automatyka domowa
dzięki centralom alarmowym NeoGSM-IP

NeoGSM-IP i **NeoGSM-IP-64** to nowoczesne centrale alarmowe z funkcjami automatyki domowej. Urządzenia są przeznaczone do domów jednorodzinnych, mieszkań, małych obiektów komercyjnych i dla użytkowników, którzy cenią sobie prostą i intuicyjną obsługę oraz pełną kontrolę nad systemem zarówno w domu, jak i poza nim. Można obsługiwać centralę i sterować systemem na wiele sposobów. W domu można używać w tym celu paneli dotykowych, smartfonu, tabletu lub pilotów radiowych. Poza domem system skomunikuje się z użytkownikiem przez sieć GSM lub Internet. Smartfon lub tablet stanowi centrum kontroli zarówno w domu, jak i w dowolnym innym miejscu na świecie. Aplikacja mobilna RopamNeo jest dostępna w wersjach dostosowanych do systemów operacyjnych Android oraz iOS. Obsługuje zarówno 6-calowe smartfony, jak i tablety o przekątnej ekranu przekraczającej 10 cali.

Opisywane centrale służą do budowy systemów alarmowych chroniących domy. Można je rozbudować i dostosować do większości typowych instalacji alarmowych. Do centrali można podłączyć dowolne czujki i sygnalizatory – w zależności od indywidualnych wymagań użytkownika dotyczących funkcjonalności i estetyki.

W sytuacji alarmowej centrala powiadamia użytkownika i informuje o źródle zagrożenia. Informacje są przekazywane w czasie rzeczywistym w formie SMS-a, komunikatu głosowego lub powiadomienia PUSH do aplikacji RopamNeo. Ponadto możliwe jest wysyłanie e-maili. Dzięki różnym typom powiadomień można je dopasować do preferencji użytkownika.

Centrala pozwala na stworzenie systemu automatyki domowej, dzięki któremu można sterować urządzeniami zainstalowanymi w domu, korzystając z paneli dotykowych lub aplikacji RopamNeo. Można na przykład sterować bramą wjazdową czy garażową, roletami, oświetleniem. Ponadto centrala umożliwia stworzenie typowych schematów lub harmonogramów sterowania, np. automatyczne włączanie oświetlenia po wejściu użytkownika do domu, sterowanie pompami systemu centralnego ogrzewania i wentylacją. Dzięki integracji funkcji alarmowych i automatycznego sterowania można wykorzystać czujki alarmowe jako czujniki w systemie automatyki domowej, np. czujniki obecności do sterowania oświetleniem, ogrzewaniem, roletami.

System ma także funkcję regulacji temperatury wewnątrz pomieszczeń zgodnie z zaplanowanymi, podanymi w kalendarzu nastawami temperatury. Pomiar temperatury jest dokonywany za pomocą czujników przewodowych lub bezprzewodowych. Elementy regulacyjne są dostępne w graficznym menu w panelach dotykowych i w aplikacji mobilnej.

System wyróżnia się nie tylko funkcjonalnością, ale też niskimi kosztami utrzymania. Urządzenia komunikują się przez przewodową lub bezprzewodową sieć IP, a zapasowym łączem jest modem GPRS z kartą SIM. Zasilacze o wysokiej sprawności energetycznej gwarantują niskie zużycie energii, a akumulatory rezerwowe mają dużą trwałość dzięki termicznej kompensacji napięcia ładowania akumulatorów.

Bezpośr. inf. Ropam Elektronik
www.ropam.com.pl
www.ochronadladomu.pl

Lepsze zabezpieczenie danych dzięki rejestratorom sieciowym NOVUS

z serii NVR 6000

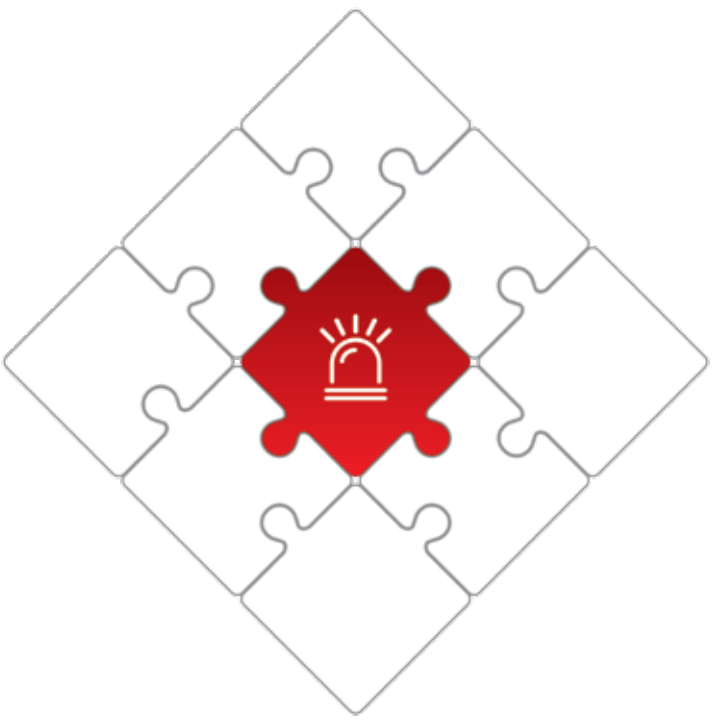
Oprogramowanie układowe w nowej wersji 1.4.1, stosowane w kolejnych modelach **rejestratorów sieciowych z serii 6000**, zapewnia wyższy poziom bezpieczeństwa danych oraz wzbogaca urządzenia w szereg nowych funkcji.

Połączenie sieciowe z aplikacjami klienckimi pracującymi w systemie operacyjnym Windows jest szyfrowane. Wymaga to aktualizacji aplikacji NMS do wersji 1.44 oraz aplikacji NVR-6000 Viewer do wersji 3.4.5. Konfiguracja rejestratora pozwala na szyfrowanie zapisu na dysku twardym, które uniemożliwia odczytanie go przez osoby nieuprawnione, np. za pomocą aplikacji do odczytu danych na dyskach twardych. Kolejnym elementem poprawiającym bezpieczeństwo systemu jest szyfrowanie eksportowanych nagrań zapisywanych z rozszerzeniem .dat. Aby odczytać zarchiwizowane dane, należy podać hasło ustanowione podczas eksportu. Zwieńczeniem nowych funkcji zabezpieczających jest dodanie obsługi protokołu 802.1x wykorzystywanego w sieciach do uwierzytelniania urządzeń.

Do rejestratorów można przesyłać strumienie RTSP z różnych źródeł, również z innych rejestratorów z serii 6000, co umożliwia tworzenie wyniesionych punktów nadzoru bez konieczności stosowania komputerów PC. Do funkcji analizy treści obrazu dodano funkcję odbierania zdefiniowanych stanów alarmowych, dotyczących liczenia ludzi oraz wykrywania tłumu. System powiadamiania został wzbogacony w połączenie logiczne detekcji ruchu oraz aktywacji wejścia alarmowego rejestratora. Również w przypadku połączenia za pomocą serwera P2P urządzenia pokazują stan połączenia z serwerem.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Integracja systemu RACS 5
z centralami alarmowymi Galaxy



System **RACS 5** został zintegrowany z centralami alarmowymi z serii **Galaxy Dimensions** firmy Honeywell. Uruchomiony na serwerze systemu kontroli dostępu wirtualny kontroler zapewnia komunikację z centralą alarmową Galaxy za pośrednictwem sieci LAN. Możliwe jest sterowanie strefami alarmowymi centrali Galaxy oraz sprawdzanie ich stanu za pomocą terminali dostępu. Sterowanie strefami alarmowymi może odbywać się za pomocą identyfikatorów, przycisków funkcyjnych, przycisków podłączonych do linii wejściowych, a także zdalnie, z poziomu oprogramowania zarządzającego systemem. Zdarzenia, które wystąpiły w systemie alarmowym, są na bieżąco prezentowane w oprogramowaniu systemu kontroli dostępu i rejestrowane w jego bazie danych. Systemem alarmowym można sterować i monitorować jego stan, korzystając w tym celu z trybu tekstowego lub graficznego – z tzw. map systemu. W reakcji na wybrane zdarzenia zachodzące w systemie alarmowym system kontroli dostępu może automatycznie podejmować wcześniej określone akcje. Uprawnienia do sterowania systemem alarmowym są określane na tych samych zasadach, co wszystkie inne typy funkcji dostępnych w systemie RACS 5. Integracja systemu alarmowego Galaxy z systemem kontroli dostępu RACS 5 zwiększa liczbę dostępnych metod sterowania strefami alarmowymi. Dzięki niej zarówno monitorowanie, jak i użytkowanie obydwu systemów jest możliwe przy użyciu oprogramowania systemu kontroli dostępu oraz jego terminali.

Bezpośr. inf. ROGER

Księga gości
w systemie RACS 5

Oprogramowanie systemu **RACS 5** powiększono o **moduł programowy przeznaczony do obsługi gości**. W systemie RACS 5 goście stanowią osobną kategorię użytkowników i są obsługiwani inaczej niż inni. Proces obsługi gościa rozpoczyna się od zarejestrowania go w systemie za pomocą specjalnego kreatora. Za jego pomocą wprowadza się do systemu dane personalne i inne dane, które dotyczą gościa, a także tworzy identyfikator z uwzględnieniem jego uprawnień. Jeżeli odwiedzający był już wcześniej zarejestrowany w systemie, możliwe jest zaimportowanie jego danych osobowych, co upraszcza obsługę w przypadkach osób często odwiedzających dany obiekt. Po zakończeniu rejestracji dane zostają przesłane do systemu i można rozpocząć wizytę. Udostępniony gościowi identyfikator ma termin ważności, po którego upływie traci uprawnienia. Identyfikator może również stracić uprawnienia automatycznie, w momencie przejścia gościa przez wybrane, określone w ustawieniach systemu jako punkt końcowy wizyty przejście. W miejscu opisu wizyty jest pole przeznaczone na komentarz, w którym obsługa obiektu może opisać dodatkowe okoliczności, które mają związek z wizytą. Oprogramowanie systemu umożliwia szczegółowe raportowanie wizyt. Raporty mogą być eksportowane do plików o popularnych formatach (PDF, DOCX, TXT, XLSX). Obsługa gości w systemie RACS 5 jest realizowana z wykorzystaniem przeznaczonego do tego celu modułu programowego VISO o nazwie *Księga gości*, który jest oferowany jako dodatkowy licencjonowany element oprogramowania systemu. Goście mogą być obsługiwani także za pomocą standardowej, bezpłatnej wersji systemu RACS 5, lecz w tym przypadku część funkcji przeznaczonych do ich obsługi jest niedostępna, a te, które są, wymagają większych kompetencji od operatora programu.

Bezpośr. inf. ROGER

Rejestrator XVR7104E-4KL-X

do niewielkich wizyjnych systemów dozorowych

XVR7104E-4KL-X to profesjonalne urządzenie rejestrujące wykorzystywane w niewielkich systemach nadzoru wizyjnego. Należy do innowacyjnej serii samoadaptacyjnych rejestratorów pięciosystemowych Pro marki **Dahua**, które umożliwiają płynną i dynamiczną rejestrację, dzięki czemu zapewniają wiarygodną identyfikację i skuteczną ochronę. Rejestrator XVR7104E-4KL-X ma cztery kanały, do których mogą być podłączone dowolne kamery CVBS/AHD/HD-CVI/HD-TVI/IP, oraz cztery dodatkowe kanały dla kamer IP (może obsługiwać osiem kanałów wizyjnych jednocześnie). Może współpracować z kamerami, które generują obraz o rozdzielczości 8 Mpx (w przypadku systemu HDCVI i IP) lub 5 Mpx (AHD/HDTVI). Ma funkcje HDCVI-IoT (to kompleksowy system łączący obraz, dźwięk oraz dane z informacjami z czujników, np. z alarmami, z informacjami dotyczącymi temperatury i wilgotności). Pozwala w porę ostrzec o potencjalnym zagrożeniu, a dodatkowo operator może wzrokowo zweryfikować dany alarm. Rejestrator ma innowacyjną funkcję zdalnego dostępu do menu OSD kamer za pomocą wbudowanego systemu operacyjnego i techniki CoC (Control over Coax). Okno, w którym można skonfigurować kamerę, jest wywoływane przez użytkownika z wykorzystaniem myszy i opcji sterowania systemem PTZ. Zdalna modyfikacja ustawień kamery nie wymaga dodatkowych połączeń przewodowych ani fizycznej ingerencji w istniejące struktury systemu nadzoru. Integracja systemu z drukarkami fiskalnymi daje wiele korzyści. Przede wszystkim umożliwia ograniczenie w sklepach strat spowodowanych kradzieżami towarów lub fałszywymi transakcjami. Na bieżąco mamy dostęp do danych dotyczących sprzedaży oraz profilu nabywcy. Połączenie danych fiskalnych oraz danych z zaimplementowanego w kamerach Dahua systemu analizującego treść obrazu pozwala na uzyskiwanie informacji o liczbie klientów, liczbie transakcji czy też wydajności obsługi.

Bezpośr. inf. Robert Sienkiewicz
Dahua Technology Poland
Opracowanie: Redakcja

Kamera IPC-PDB4830-B360
firmy Dahua Technology

Mimo że korzyści płynące z połączenia kilku kamer w jedną nie są już nikomu obce, dotychczas stosowane kamery panoramiczne były czterokrotnie większe i cięższe od pojedynczych kamer. Najnowsza kamera wieloprzetwornikowa z naszej oferty to **IPC-PDB4830-B360** nie ma tej wady. Jest wyposażona w cztery **przetworniki Sony** STARVIS 1/2,8" o rozdzielczości Full HD. Do wyboru mamy dwie wersje obiektywów, o ogniskowej 2,8 mm lub 3,6 mm, z których każdy można dostosować do obserwowanej sceny i w efekcie monitorować obszar w polu widzenia obejmującym 360°. W przypadku wyboru ogniskowej 3,6 mm można objąć dozorem teren o szerokości ponad 100 m.

Zaawansowana funkcja analizy treści obrazu wykrywa przekroczenie linii czy wtargnięcie intruza do wyznaczonej strefy, dzięki czemu kamera IPC-PDB4830-B360 świetnie sprawdzi się na parkingach. Klasa szczelności IP67 i wandaloodporności IK10 umożliwia zamontowanie jej nawet w tak newralgicznych miejscach jak więzienne place czy korytarze.

Bezpośr. inf. Ewelina Pułka
Dahua Technology Poland

Nowy zasilacz do kontrolerów KD

Oferujemy nowy produkt firmy **MERAWEX** – zasilacz **KDH-ZAS12/6/17** o napięciu nominalnym 13,8 V_{DC}, przeznaczony przede wszystkim do kontrolerów KDH-KS3024-IP ze względu na wydajność prądową wynoszącą 6 A, która umożliwia zasilanie modułu kontrolera, czytników oraz czterech zamków, z których każdy może charakteryzować się poborem prądu wynoszącym nawet 1 A. Zasilacz ma trzy wyjścia. Pierwsze z nich służy do zasilania zamków i jest zabezpieczone przed zwarciem za pomocą pozystora. Drugie wyjście – o wydajności 1 A (również zabezpieczone za pomocą pozystora) – jest przeznaczone do zasilania modułu kontrolera wraz z czterema czytnikami. Trzecie wyjście służy do podłączania akumulatora.

Sposób instalacji i konserwacji akumulatora stanowi ważną cechę tego zasilacza. Dzięki miejscu w jego obudowie oraz wydajności wyjścia przeznaczonego do jego ładowania można zainstalować w nim baterię o pojemności do 18 Ah. Umożliwia to znacznie dłuższą pracę kontrolera, czytników i zamków po zaniku zasilania sieciowego. Jest to pierwszy w naszej ofercie model przeznaczonego do kontrolerów KD zasilacza z akumulatorem o pojemności do 18 Ah. Instalatorzy i klienci często pytali o możliwość wydłużenia czasu pracy systemu KD przy braku zasilania z sieci energetycznej, dlatego ten nowy model powinien cieszyć się dużą popularnością. Do tej pory do zasilania kontrolerów przeznaczonych do obsługi czterech drzwi oferowaliśmy model APSAAT4, ale współpracuje on tylko z akumulatorem 7 Ah. Przyczyniało się to do skrócenia czasu pracy systemu po zaniku napięcia sieciowego.

Zasilacz buforowy KDH-ZAS12/6/17 ma na tylnej ściance otwory umożliwiające montaż kontrolerów KaDe z serii KS2000 oraz KS3000 i Kantech KT-1. W przypadku kontrolerów obsługujących jedne drzwi czas pracy po zaniku napięcia sieciowego wydłuży się bardzo znacznie. Czas ten można obliczyć, sumując prądy obciążające zasilacz i korzystając z odpowiedniego wzoru na czas rozładowania akumulatora. Podczas korzystania z akumulatora napięcie jest kontrolowane. Akumulator jest odłączany po osiągnięciu bezpiecznego poziomu wynoszącego 10,5 V, umożliwiającego jego powtórne naładowanie.

Zasilacz jest wyposażony w moduł monitorujący stan jego pracy i udostępnia sygnały NO/NC informujące o zaniku napięcia sieciowego i przejściu w tryb pracy z wykorzystaniem akumulatora. Sygnalizowany jest także zbyt niski poziom napięcia na akumulatorze. Wyjścia NO/NC podobnie jak styki czujnika otwarcia drzwiczek obudowy, należy podłączyć do wolnych wejść linii dozorowych w kontrolerze i opisać ich funkcje w nazwach linii.

Polecam ten produkt do projektów związanych z kontrolą dostępu.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING
Opracowanie: Redakcja

Unowocześniona seria kamer kopułkowych Q mini

firmy Hanwha Techwin

W sierpniu bieżącego roku **Hanwha Techwin** zaprezentowała swoją unowocześnioną serię kamer kopułkowych **Q mini**. Nowe kamery mają zaledwie 99 mm średnicy. Zastosowano w nich nowe przetworniki, dzięki czemu rozdzielczość wzrosła do 5 Mpx.

Kamery z serii Q mini mają funkcje, dzięki którym użytkownicy końcowi mogą czerpać maksimum korzyści z wizyjnego systemu dozorowego.

Nowe kamery są o 40% mniejsze od poprzednich modeli. Zredukowanie wielkości nie wpłynęło jednak na ich możliwości. Nowe minikopułki zapewniają rzeczywiste korzyści użytkownikom końcowym, a w szczególności sprzedawcom detalicznym, którzy oczekują zainstalowania estetycznych kamer na ścianach i sufitach swoich sklepów. W nowej serii zastosowano kodek Wisestream II, który dotychczas był spotykany w serii X.

W przypadku nowej serii kamer kopułowych można bezpłatnie korzystać z funkcji liczenia osób, zarządzania kolejkami oraz tworzenia map cieplnych. Umożliwia to sprzedawcom ocenę skuteczności funkcjonowania sklepu na podstawie liczby odwiedzin oraz sprzedaży. Sprzedawcy mogą wykorzystać dane pochodzące z systemu, aby ocenić wpływ promocji i innych działań marketingowych na liczbę osób odwiedzających sklep, jak również zoptymalizować zasoby ludzkie tak, aby najefektywniej rozlokować personel sklepowy w godzinach największego ruchu klientów.

Nowe minikopułki zostały już zintegrowane z oprogramowaniem Retail Insight, niedawno uruchomionym systemem do analityki biznesowej, który wykorzystuje sieciową aplikację do zliczania osób, zarządzania kolejkami i tworzenia map cieplnych. Można na przykład wykorzystywać mapy cieplne ze wszystkich umieszczonych w sklepie kamer typu rybie oko (QNF-8010), a wyniki przedstawić w formie graficznej prezentacji natężenia ruchu klientów w sklepie. Oprogramowanie to jest w stanie zebrać dane z nawet 500 kamer, dzięki czemu może być wykorzystane w dużych sieciach handlowych. Wygenerowane dane mogą przyczynić się do wzrostu sprzedaży dzięki analizie układu sklepu oraz do zmniejszenia kosztów operacyjnych dzięki umożliwieniu dobrania odpowiedniej liczby pracowników.

Kamery należące do serii Q mini mają wiele funkcji, które umożliwiają dopasowanie ich do warunków panujących w obiektach, m.in. korekcji zniekształceń obiektywu (LDC) i rozszerzania zakresu dynamiki (WDR) do 120 dB. Ponadto kamery QND-8011 i QND-8021 mają wyjście wizyjne HDMI, które umożliwia wyświetlanie obrazów na monitorze umieszczonym w przestrzeni publicznej sklepu.

Więcej informacji na ten temat znajduje się pod adresem www.hanwha-security.eu.

Bezpośr. inf. Sylwester Krupa
Hanwha Techwin
Opracowanie: Redakcja

Firmy Fujifilm i Videotec łączą siły, aby stworzyć wizyjne systemy dozorowe dalekiego zasięgu

Firmy **Fujifilm** i **Videotec** informują o nawiązaniu współpracy w celu integracji swoich najlepszych produktów i stworzenia nowych, innowacyjnych rozwiązań w dziedzinie wizyjnych systemów dozorowych dalekiego zasięgu. Systemy te będą wykorzystywane do ochrony obiektów infrastruktury krytycznej, sieci transportowych, w tym lotnisk, portów, autostrad, a także granic państwowych. Znajdą zastosowanie także w instalacjach dozorowych związanych z ochroną środowiska.

W skład zintegrowanego punktu dozorowego wchodzi wysokiej klasy kamera **SX800** firmy Fujifilm umieszczona w obudowie **ULISSE MAXI** zainstalowanej na głowicy PTZ firmy Videotec. Obudowa ULISSE MAXI ma sztywną konstrukcję i na tyle duże rozmiary, że można w niej instalować kamery IP z dużymi i ciężkimi obiektywami zmiennoogniskowymi. Mechanizm PTZ jest konstrukcyjnie dostosowany do precyzyjnego pozycjonowania tak dużego i ciężkiego zestawu. Silniki napędzające ten mechanizm mają na tyle dużą moc, że są w stanie pokonać obciążenia powodowane przez silny wiatr. Przednia szyba obudowy jest wyposażona w wycieraczkę, więc możliwa jest obserwacja z dużej odległości i dostrzeżenie szczegółów nawet w bardzo złych warunkach pogodowych.

Obiektyw kamery SX800 ma ogniskową regulowaną w zakresie od 20 mm do 800 mm, co daje krotność przy regulacji równą 40x. Dodatkowo obraz może być powiększony elektronicznie 1,25x, co odpowiada dalszemu wydłużeniu ogniskowej obiektywu do 1000 mm. Wbudowany stabilizator obrazu pozwala na ograniczenie wpływu drgań i wibracji punktu kamerowego na skutek złej pogody i silnego wiatru. Nawet wtedy, gdy korzysta się z najdłuższej dostępnej ogniskowej, czyli w warunkach, w których wpływ nawet niewielkich drgań podstawy kamery jest łatwo zauważalny, punkt kamerowy umożliwia skuteczną obserwację obiektów znajdujących się w dużej odległości

Kamera SX800 ma przetwornik obrazu odznaczający się wysoką czułością i niskim poziomem

szumów, dzięki czemu uzyskuje się czytelny obraz nawet w złych warunkach oświetleniowych. Dzięki funkcji redukcji wpływu mgły na jakość obrazu można zastosować kamerę SX800 w zanieczyszczonym, mało przejrzystym środowisku. Uzyskiwane obrazy zachowują czytelność pomimo zadymienia lub mgły.

– Nasza głowica ULISSE MAXI w połączeniu z kamerą Fujifilm SX800 pozwala na stworzenie obrotowego punktu kamerowego zdolnego sprostać nawet najtrudniejszym wyzwaniom. Uzyskiwany obraz ma wysoką jakość, jest stabilny i czytelny nawet podczas obserwacji prowadzonych w bardzo złych warunkach środowiskowych. W ten sposób spełniamy oczekiwania nawet najbardziej wymagających użytkowników wizyjnych systemów dozorowych o dużym zasięgu – powiedział Alessio Grotto, dyrektor firmy Videotec.

Produkty można obejrzeć na stronach www.fujifilm.eu/sx800 (kamera) i https://www.videotec.com/cat/en/products/telecamere-e-unita-ptz/telecamere-e-unita-ptz-ulisse/ulisse-maxi-netcam/ (głowica PTZ).

Fujifilm Optical Devices Europe
tel.: +49 2821 7115 400
e-mail: cctv_eu@fujifilm.com
www.fujifilm.eu/fujinon

Videotec
Martina Panighel (kontakt medialny)
martina.panighel@videotec.com
sales@videotec.com
www.videotec.com

Bezpośr. inf. Videotec
Tłumaczenie: Andrzej Walczyk

Smart IR w kamerach serii 6000
marki NOVUS

Funkcja **Smart IR** w wersji sprzętowej jest dostępna w należących do serii 6000 kamerach **NVIP-5H-6412M/F, NVIP-5H-6422M/F, NVIP-5VE-6401/F** oraz **NVIP-5VE-6402M/F**. Smart IR dynamicznie reguluje intensywność świecenia wbudowanego w kamerę promiennika podczerwieni w zależności od odległości kamery od obserwowanego obiektu. Dzięki temu obraz nie jest prześwietlony, a obiekty są wyraźnie widoczne nawet w małej odległości od kamery. Funkcja ta jest rekomendowana do scen o dalekiej perspektywie, w których obserwowane obiekty zbliżają się do kamery z pracującym promiennikiem. Automatyczna, dynamiczna zmiana mocy świecenia diod w zależności od obserwowanej sceny wynika z zastosowania zaawansowanych podzespołów wspomagających pracę diod IR oraz algorytmów realizowanych przez wysokiej klasy procesor. Możliwe jest także ręczne ustawienie poziomu mocy diod IR. W celu pokazania dynamiki działania tej funkcji zachęcamy do obejrzenia przygotowanego filmu demonstracyjnego, który jest dostępny na kanale YouTube firmy AAT HOLDING (https://www.youtube.com/watch?v=jpnJ0A-VEgA).

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Zasilacz awaryjny PowerWalker Smart PoE UPS

BlueWalker wprowadza lokalny zasilacz awaryjny **PowerWalker** do urządzeń PoE. Awaria sieci energetycznej nie wyłączy już twoich kamer.

PowerWalker Smart PoE UPS to zasilacz awaryjny wyposażony w baterie litowo-jonowe o pojemności 36,5 Wh. Dostarcza on stałego napięcia 48 V w celu zasilania urządzeń o mocy nie przekraczającej 15,4 W metodą PoE. Najczęściej tymi urządzeniami są kamery przemysłowe, sieciowe punkty dostępowe lub przełączniki, które pobierają energię za pośrednictwem kabla sieciowego. Nowy UPS marki PowerWalker ma interfejs PoE zgodny ze standardami 802.3af/802.3at.

PowerWalker Smart PoE UPS może być wykorzystywany do zdecentralizowanego zasilania awaryjnego w systemach dozoru wizyjnego. Sprawdzi się wszędzie tam, gdzie liczy się przede wszystkim ciągłość nagrań w przypadku zaniku zasilania lub awarii infrastruktury sieciowej (podczas pożaru, rozległego blackoutu, ataku terrorystycznego, działania złodzieja w celu zatarcia śladów itp.).

W przypadku odcięcia kamery od przełącznika PoE zapewniającego jej zasilanie urządzenie PowerWalker zapewnia podtrzymanie zapisu materiału wizyjnego nawet przez kilka godzin. Obraz będzie zapisywany na karcie microSD umieszczonej w kamerze. Smart PoE UPS sprawdzi się także w systemach dozorowych w budynkach użyteczności publicznej, na dworcach kolejowych, stacjach metra, w bankach, centrach handlowych itp.

Więcej szczegółowych informacji znajduje się na stronie https://powerwalker.com.

Bezpośr. inf. Impakt

Roboty patrolujące

nowy etap rozwoju ochrony fizycznej

Ochrona fizyczna połączona ze wsparciem technicznym osiąga nowy etap rozwoju. Od tej pory możliwe jest korzystanie z mobilnego systemu dozorowego wykorzystującego sztuczną inteligencję.

Dzięki firmie **Security Robot Guard Systems w Polsce** dostępne będą **roboty patrolujące**, które odpowiadają dzisiejszym potrzebom. Roboty są przeznaczone do wspierania pracowników ochrony w wykonywaniu najbardziej monotonnych, lecz często bardzo ważnych zadań związanych z patrolowaniem chronionych obszarów. Mogą być wyposażone w czujniki temperatury, dymu lub gazu, kamery termowizyjne, systemy rozpoznawania tablic rejestracyjnych lub twarzy. Mogą służyć jako mobilne recepcje i urządzenia wskazujące drogę do sklepu, np. w galerii handlowej. Sprawdzą się także jako strażnicy na osiedlach, potrafiący otworzyć szlaban, kiedy podjedzie do niego służba ratownicza na sygnale, wskazać gościom drogę lub połączyć się z mieszkaniem określonego lokatora w celu powiadomienia go o wizycie.

Roboty patrolujące są produkowane w wersjach przeznaczonych do pracy na płaskich podłogach wewnątrz obiektów, na drogach utwardzonych na zewnątrz obiektów, a także na duktach trawiastych lub ziemnych. Utrzymują połączenie z Alarmowym Centrum Odbiorczym, stacją monitorowania lub – w przypadku krótkotrwałego braku dostępu do sygnału wi-fi lub GSM podczas patrolowania – działają w trybie off-line, a po odzyskaniu łączności informują Alarmowe Centrum Odbiorcze, jeżeli doszło do jakichś incydentów.

Roboty wejdą do stałej sprzedaży **w pierwszym kwartale 2020 roku**, jednak już dziś zapraszamy zainteresowanych do skontaktowania się z nami w celu zapoznania się z ofertą i poznania bliżej zagadnień związanych z robotyką w ochronie.

Firma Security Robot Guard Systems jest nowym podmiotem na rynku, ale stworzyli ją profesjonaliści, którzy działają w branży ochrony fizycznej, nadzoru wizyjnego i zabezpieczeń technicznych już od ponad 20 lat. Doświadczenie zawodowe, zaangażowanie i znajomość rynku zabezpieczeń umożliwiły tworzenie urządzeń do niedawna uważanych za futurystyczne.

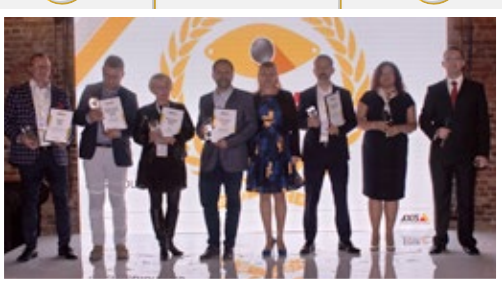
Bezpośr. inf. Grzegorz Wyszyński
Security Robot Guard Systems
tel. kom.: +48 601 755 100
ul. Modlińska 51/515
03-199 Warszawa
www.srgs.pl
e-mail: biuro@srgs.pl

SRGS SECURITY ROBOT GUARD SYSTEMS

Axis Partners Day 2019

podsumowanie

24 września, w ramach **Axis Partners Day 2019**, odbyło się kolejne spotkanie partnerów biznesowych firmy Axis Communications. Tym razem impreza miała miejsce w Warszawie, w starej praskiej kamienicy przy ulicy Brzeskiej 22. Licznie przybyli goście zostali zaproszeni do sali konferencyjnej mieszczącej się na parterze budynku. Po otwarciu spotkania dokonanym przez Dagmarę Pomirską na scenie zaprezentował się zespół polskich pracowników firmy Axis Communications oraz goście ze Szwecji. Następnie, po wręczeniu nagród dla najaktywniejszych partnerów biznesowych, wygłoszono kilka prelekcji. Zaprezentowano nowości w ofercie firmy i omówiono ciekawe rozwiązania techniczne, takie jak AXIS Audio, czyli sieciowe systemy do transmisji dźwięku. Nie zabrakło informacji marketingowych i handlowych. Wyjaśnione zostały aspekty prawne wynikające z wdrożenia RODO i ich wpływ na projektowanie wizyjnych systemów dozorowych.



Na uwagę zasługiwała bardzo dobra organizacja imprezy. Nikt się nie nudził, goście byli cały czas absorbowani przez organizatorów. Na pierwszym piętrze, w obszernej sali wystawowej, znajdowały się stoiska, na których prezentowano sprzęt i oprogramowanie firmy Axis Communications, a także produkty zaprzyjaźnionych kooperantów. Atrakcyjnym pomysłem było zorganizowanie czegoś na kształt wycieczek z przewodnikiem. Goście zostali podzieleni na kilkunastoosobowe grupy, którym przydzielono opiekunów. Grupy wędrowały rotacyjnie od stoiska do stoiska, gdzie przewodnicy objaśniali budowę i zastosowanie prezentowanych produktów. Na koniec odbyła się prezentacja nadesłanych prac i wręczenie nagród w konkursie fotograficznym *Gdzie jest Axis?*. Liczny udział partnerów firmy Axis Communications w tym konkursie świadczy o jej dużej popularności w Polsce.

Andrzej Walczyk
Redakcja

25 lat istnienia Polskiej Izby Ochrony

i 20. konferencja branży ochrony

W dniach **17–18 października 2019** r. w hotelu Magellan w Bronisławowie odbyła się dwudziesta konferencja **Polskiej Izby Ochrony** połączona z jubileuszem **25-lecia** istnienia Izby. W spotkaniu wzięło udział ponad 170 osób oraz kilkanaście firm partnerskich, które zaprezentowały swoje rozwiązania i produkty w sali wystawienniczej i podczas warsztatów.

Konferencja rozpoczęła się od powitania gości przez prezesa zarządu Marcina Pyclika i podziękowań za pracę dla wszystkich współpracowników Polskiej Izby Ochrony.

Podczas konferencji omówiono m.in. zdarzenia mające wpływ na cyberbezpieczeństwo w przedsiębiorstwie, systemy informatyczne do zarządzania środkami trwałymi w branży zabezpieczeń i rozwiązania dla branży ochrony działające w chmurze.

W trakcie wystąpień poświęconych nowym przepisom prawa pracy omówiono m.in. warunki legalnego zatrudniania cudzoziemców, a także warunki przystąpienia do programu pracowniczych planów kapitałowych i korzyści z nich wypływające.

Brak chętnych do pracy i wzrost kosztów zatrudnienia pracowników zajmujących się ochroną fizyczną powoduje coraz większe zainteresowanie postępem w dziedzinie techniki. W części konferencji poświęconej nowym produktom i rozwiązaniom przedstawiono korzyści wynikające z zastosowania zdalnej ochrony obiektu, która umożliwia redukcję kosztów zatrudnienia pracowników ochrony i stałe monitorowanie obiektu, a także zwiększa możliwości zabezpieczenia obiektu. Najnowsza analiza obrazu w kamerach do nadzoru wizyjnego i wykorzystanie w nich algorytmów sztucznej inteligencji umożliwia dokładne rozpoznawanie obiektów nawet w nocy, rozpoznawanie twarzy i określonych zachowań, dzięki czemu przyczynia się do zmniejszenia liczby fałszywych alarmów.

W trakcie konferencji omówiono również przyszłość zabezpieczeń antyterrorystycznych i tendencje w ich rozwoju. Na zakończenie części wykładowej pierwszego dnia konferencji odbyła się debata na temat przyszłości branży ochrony w obliczu współczesnych

zagrożeń i antyterrorystycznych zabezpieczeń budynków użyteczności publicznej.

Z okazji 25-lecia istnienia Polskiej Izby Ochrony odbyła się uroczysta gala. Nie zabrakło gratulacji, słów uznania oraz życzeń z okazji tak wspaniałego jubileuszu. Rozdano pamiątkowe statuetki. Uroczystość uświetnił występ piosenkarki Haliny Frąckowiak. Jubileuszowa impreza była okazją do spotkania się z przedstawicielami firm, z którymi Polska Izba Ochrony współpracuje od wielu lat. W uroczystej gali wzięli udział również byli członkowie zarządu i założyciele PIO.

W 2007 roku Polska Izba Ochrony powołała Fundację Pomocy Pracownikom Ochrony i Ich Rodzinom „Ochrona i Pomoc". Podczas gali odbyła się aukcja na rzecz fundacji.

Drugiego dnia odbyły się warsztaty partnerów technologicznych i losowanie nagród.

Serdecznie dziękujemy za zaproszenie, a zarządowi Polskiej Izby Ochrony życzymy wszystkiego najlepszego, sukcesów i kolejnych 25 lat owocnych działań dla branży ochrony!

Zapraszamy do obejrzenia fotorelacji z konferencji na stronie https://www.zabezpieczenia.com.pl/fotogalerie.

Ela Końka

Projektanci docenili nowości na jesiennej edycji SPIN

W dniach **25–26 września w Zakopanem** po raz siedemnasty spotkali się projektanci z południowej i centralnej Polski, by zdobywać wiedzę i nawiązać kontakty z dostawcami technologii w branży niskich prądów.

17. SPIN był wyjątkowy pod względem debiutów. Po raz pierwszy na udział zdecydowały się firmy Commscope, Dallmeier, Dormakaba, Samsung, Yamaha, Alter, Q07 i SMAY. Partnerzy, którzy wzięli udział w SPIN-ie ponownie, to: Axxonsoft, Grupa Romi, Corning, TP-link, APA Group, Assa Abloy, BCS, Dipol, GiP, Helukabel, Mercor, ROGER, Zettler, Gazex, Winkhaus, Eaton, Extreme Networks, Veracomp, Optex, S-Cabling, Batna Anteny24, ecVISION, UTC.

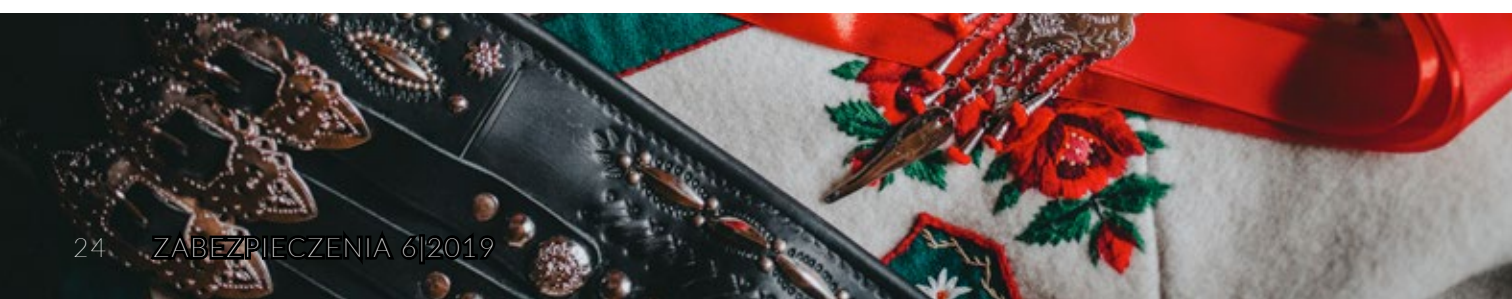
– Bardzo nas cieszy tak duże zainteresowanie nowych firm. Świadczy ono o tym, że nieustannie kluczowy pozostaje bezpośredni kontakt z projektantami, osobami mającymi wymierny wpływ na kształt projektów. A SPIN ten kontakt umożliwia – powiedziała Magdalena Skórkiewicz-Foltyn, dyrektor ds. rozwoju w firmie Lockus.

Nie mniej istotny jest fakt, iż w SPIN-ie biorą udział firmy, które od lat są partnerami i doceniają to, jak on ewoluuje. Organizator przywiązuje wagę do tego, by miały one okazję do kontaktu z innymi firmami i projektantami.

Szerzenie wiedzy oraz integracja branży to najważniejsze cele SPIN-u. Nowością podczas tej edycji były zorganizowane w przeddzień wydarzenia warsztaty z firmą TP-link. W trakcie popołudniowej sesji uczestnicy mieli okazję poznać przełączniki zarządzalne oraz rozwiązania biznesowe.

Bezpośr. inf. Lockus

Zapraszamy do obejrzenia fotogalerii na stronie internetowej
https://www.zabezpieczenia.com.pl/fotogalerie



Systemy zabezpieczeń mechanicznych i kontroli dostępu w obiektach infrastruktury krytycznej

podsumowanie

W **październiku br. w Warszawie** odbyła się druga edycja szkolenia *Systemy zabezpieczeń mechanicznych i kontroli dostępu w obiektach infrastruktury krytycznej*. Szkolenie zorganizowała firma **Assa Abloy Poland** we współpracy z Siecią Badawczą ŁUKASIEWICZ – **Instytutem Mechaniki Precyzyjnej** i firmą **Energo-Security Serwis**.

W spotkaniu wzięło udział ponad 40 osób odpowiedzialnych za bezpieczeństwo w obiektach infrastruktury krytycznej. Uczestników powitali prof. dr hab. inż. Jerzy Jeleńkowski – zastępca dyrektora ds. naukowych w instytucie oraz Grzegorz Korzeniowski – dyrektor zarządzający w firmie Assa Abloy Poland.

Przedstawiciele Sieci Badawczej ŁUKASIEWICZ – Instytutu Mechaniki Precyzyjnej omówili przepisy i normy dotyczące mechanicznych zabezpieczeń obiektów infrastruktury krytycznej. Przedstawiono również zadania instytutu w zakresie badań i certyfikacji wyrobów stanowiących mechaniczne środki ochrony dostępu, takie jak drzwi, zamki, wkładki, kraty.

W ramach struktury organizacyjnej instytutu funkcjonuje Laboratorium Badań Mechanicznych Urządzeń Zabezpieczających i Lekkich Przegród Budowlanych, które posiada aktualny certyfikat akredytacji nr AB 035 wydany przez Polskie Centrum Akredytacji.

Współorganizator konferencji – Sławomir Goździecki z firmy Energo-Security Serwis – omówił zasady projektowania zabezpieczeń mechanicznych i budowlanych stosowanych w obiektach infrastruktury krytycznej, praktyczne rozwiązania i najczęściej popełniane błędy. Podał przykłady dobrych i złych połączeń zabezpieczeń mechanicznych z systemem kontroli dostępu, systemem alarmowym, systemem sygnalizacji pożarowej i innymi systemami.

Konrad Szadkowski przedstawił rozwiązania i produkty Assa Abloy przeznaczone do zastosowania w obiektach infrastruktury krytycznej. W ofercie firmy Assa Abloy Poland znajdują się m.in. klucze, kłódki, zamki elektroniczne, wkładki bębenkowe, depozytory kluczy, system klucza głównego (*master key*) oraz system ABLOY PROTEC 2 CLIQ, który integruje rozwiązania mechaniczne i elektroniczne oraz pozwala na zdalne zarządzanie systemem zabezpieczeń również w obiektach rozproszonych. Umożliwia także kontrolę użycia kluczy w dowolnym czasie dzięki znajdującemu się w kluczu dziennikowi zdarzeń i zdalne zarządzanie prawami dostępu poszczególnych użytkowników. System ABLOY PROTEC 2 CLIQ spełnia wymagania norm PN-EN 12320 oraz PN-EN1303.

Spotkanie zakończyło się losowaniem nagród i rozdaniem upominków dla uczestników. Nasz magazyn objął patronat medialny nad szkoleniem.

Bardzo dziękujemy za zaproszenie, a firmie Assa Abloy Poland życzymy dalszych sukcesów i rozwoju. Zapraszamy do obejrzenia fotogalerii na naszej stronie internetowej (https://www.zabezpieczenia.com.pl/fotogalerie).

Bezpośr. inf. Ela Końka

Si Event Starlight Show
Special Edition
podsumowanie

W październiku br. w Folwarku Łochów odbyła się pierwsza edycja spotkania **Si Event Starlight Show Special Edition** zorganizowana przez firmę **Dahua Technology Poland** – producenta systemów zabezpieczeń. W spotkaniu wzięło udział ponad 100 integratorów systemów zabezpieczeń, a partnerem szkolenia była firma Seagate oferująca dyski twarde do wizyjnych systemów dozorowych.

Celem spotkania było przedstawienie wizji projektowania nowoczesnych systemów nadzoru wizyjnego wykorzystujących najnowsze techniki analizy treści obrazu i algorytmy sztucznej inteligencji.

Zaprezentowano kamery i rejestratory Dahua Technology wykorzystujące algorytmy sztucznej inteligencji, m.in. nowoczesne kamery IPC-HFW5442E-ZE i DH-IPC-HFW7442H-ZFR oraz rejestrator NVR5216-8P-I.

IPC-HFW5442E-ZE to nowoczesna kamera sieciowa z przetwornikiem Starlight+ o rozdzielczości 4 megapikseli odznaczającym się dużą światłoczułością. Do analizy treści obrazu wykorzystane są algorytmy sztucznej inteligencji. Kamera ma funkcję wykrywania twarzy i określa cechy obserwowanych osób, takie jak wiek, płeć, nastrój (wesołość, zdziwienie, spokój, złość, smutek, niezadowolenie, wzburzenie, strach), a także pozwala wyróżnić osoby noszące okulary lub maskę przykrywającą usta, wąsy i brodę. Ponadto kamera ma funkcje ochrony perymetrycznej poprzez detekcję obiektów, takich jak samochody i piesi.

DH-IPC-HFW7442H-ZFR ma podobne właściwości jak jej poprzedniczka, tyle że jej funkcje analityczne są bardziej zaawansowane. Zakres rozpoznawanych cech osób oraz ich ubioru jest znacznie szerszy. Ponadto algorytmy sztucznej inteligencji wykrywają próby zastąpienia twarzy jej zdjęciem. Ten model kamery odznacza się doskonalszą metodą kompresji obrazu Smart H.265+, która umożliwia redukcję pasma sieciowego i pojemności pamięci masowej o 70%.

Rejestrator NVR5216-8P-I wyróżnia się tym, że ma wbudowane funkcje analityczne opisane powyżej. Możliwa jest analiza treści obrazów z kamer pochodzących od różnych producentów.

W ofercie firmy Dahua Technology znajdują się również systemy kontroli dostępu, inteligentne systemy transportowe, systemy rozpoznawania tablic rejestracyjnych i mobilne systemy dozorowe.

Dużo uwagi poświęcono transmisji danych. Zaprezentowano dostępne w ofercie firmy przełączniki sieciowe oraz rozwiązania bezprzewodowe. W 2018 r. Dahua Technology opatentowała metodę zasilania urządzeń i jednoczesnej transmisji danych zwaną ePoE (enhanced Power over Ethernet). Metoda zastosowana w kamerach IP oraz przełącznikach sieciowych pozwala na transmisję danych i zasilanie kamer na odległość do 800 m w przypadku wykorzystania zwykłego przewodu UTP.

Gospodarze omówili również błędy, które występują na etapie projektowania i wykonania systemu nadzoru wizyjnego, oraz zasady współpracy z projektantami.

Na koniec części wykładowej odbył się konkurs wiedzy o produktach Dahua Technology i rozdanie nagród. Główną nagrodą była jazda testowa BMW i8 przez kilka dni. Spotkanie zakończyło się uroczystą kolacją i zabawą z DJ-em.

Firmie Dahua Technology Poland bardzo dziękujemy za zaproszenie i życzymy kolejnej udanej edycji spotkania.

Zapraszamy do obejrzenia fotogalerii na naszej stronie internetowej (https://www.zabezpieczenia.com.pl/fotogalerie).

Bezpośr. inf. Ela Końka

Podsumowanie konferencji Security 4.0 zorganizowanej przez firmę EBS

Rok 2019 jest wyjątkowy dla firmy **EBS**, która obchodzi **30-lecie** swojego istnienia. Z tej okazji tegoroczna konferencja **Security 4.0** również miała wyjątkowy, międzynarodowy charakter. W odróżnieniu od poprzednich (odbywających się od dziewięciu lat) wzięli w niej udział partnerzy i klienci firmy EBS zarówno z Polski, jak i z całego świata.

Konferencja Security 4.0 odbyła się 27 września. Mieliśmy okazję gościć naszych znamienitych partnerów z 26 krajów i czterech kontynentów. W sumie udział wzięło prawie 80 firm – dystrybutorów, integratorów, agencji ochrony.

Chcieliśmy, aby na konferencji poruszane były istotne zagadnienia związane ze zmianami, jakie zachodzą i będą zachodzić w najbliższych latach pod wpływem cyfryzacji, rozwoju sztucznej inteligencji oraz automatyzacji różnych procesów. Z tego powodu wypowiedzieli się przede wszystkim praktycy – Krzysztof Kuźbik (z funduszu inwestycyjnego Avallon, wieloletni wykładowca), Krzysztof Bartuszek (prezes firmy Securitas Polska), Anna Śliwoń (analityk w międzynarodowej wywiadowni gospodarczej IHS Markit, pracuje na co dzień w Wielkiej Brytanii), Daniel Kamiński (wieloletni praktyk i publicysta branżowy, obecnie sprawuje funkcję dyrektora ds. innowacji oraz członka zarządu w firmie EBS) oraz Tomasz Laudy (obecnie wiceprezes firmy EBS, który swoje kompetencje i wiedzę zdobywał w firmach Ericsson, Siemens, Orange i Roshan).

Konferencja została podzielona na pięć bloków tematycznych. Swoje produkty i rozwiązania przedstawiły firmy EBS, Orange (Paweł Dębiński), Next (Sławomir Piela), Dahua (Maciej Pietrzak) oraz Linc (Jakub Sobek) – jako partnerzy. W ostatnich

blokach głos zabrali partnerzy zagraniczni EBS-u – przedstawiciel firmy MaxiMan z RPA (właściciela największej agencji ochrony Chubb w Afryce, który wykorzystał sztuczną inteligencję w swoim systemie raportowania) oraz właściciel brazylijskiej firmy Setech opowiadający o nowej metodzie sprzedaży urządzeń (Active Track) jako usługi.

Całości dopełniły warsztaty, na których zaprezentowano nowe rozwiązania, m.in. integrację centrali EBS z elementami smart home firmy Fibaro i AV Enterprise. Odbył się też wykład przygotowany przez partnera – Polską Izbę Systemów Alarmowych.

Szczególne podziękowania należą się partnerom (firmom Fibaro, Next, Orange, Dahua, Linc, AdInfo, Security Robot Guard Systems), Instytutowi Łączności pełniącemu rolę patrona naukowego, a także partnerom honorowym (Polskiej Izbie Ochrony, Polskiej Izbie Systemów Alarmowych i Polskiemu Związkowi Pracodawców Ochrona).

Swój udział zaznaczyli również partnerzy medialni: „a&s Polska", „Zabezpieczenia" oraz alarmy.org. Doceniamy bardzo duży wkład merytoryczny wszystkich ekspertów i prelegentów.

Po części oficjalnej miała miejsce uświetniająca jubileusz firmy EBS uroczysta gala z udziałem rewelacyjnej, jak zawsze, Grupy Mo Carta.

Zapraszamy za rok!

Bezpośr. inf. EBS
Opracowanie: Redakcja

NAJWAŻNIEJSZE

WYDARZENIE 2019 r. BRANŻY SECURITY już za nami!

W dniach 18 - 21 września br., w gościnnych progach Centrum Konferencyjno-Wypoczynkowego „Pałac i Folwark Łochów", firma **POLON-ALFA S.A.** zorganizowała XXVII Ogólnopolskie Warsztaty **Sygnalizacja i Automatyka Pożarowa SAP '2019**.

Niezwykle ciekawy temat wiodący **„Dobre praktyki w zakresie bezpieczeństwa"** zgromadził rekordową liczbę czterystu pięćdziesięciu uczestników, którzy z ogromną uwagą wysłuchali referatów wygłoszonych przez m.in.: Mariusza Sobeckiego, rzeczoznawcę ds. zabezpieczeń przeciwpożarowych, Dariusza Ratajczaka - niezależnego eksperta w dziedzinie bezpieczeństwa, Grzegorza Kubickiego - wykładowcę Politechniki Warszawskiej, Ryszarda Stępkowskiego - rzeczoznawcę ds. zabezpieczeń przeciwpożarowych, Artura Litwina - przedstawiciela zachodniopomorskiego oddziału Stowarzyszenia Inżynierów i Techników Pożarnictwa, Piotra Smardza - rzeczoznawcę ds. zabezpieczeń przeciwpożarowych oraz Roberta Kuczkowskiego - inżyniera ryzyka PZU LAB S.A.

Ważnym punktem programu warsztatów było wystąpienie Mariusza Radoszewskiego, menedżera inżynierów wsparcia technicznego POLON-ALFA S.A., który zaprezentował nowe produkty, trafiające właśnie do oferty rynkowej firmy – centralę automatycznego gaszenia IGNIS 2500, pożarowy zasilacz buforowy PZB 6000, adresowalne oraz konwencjonalne sygnalizatory akustyczno-optyczne serii SAB, adresowalną i konwencjonalną czujkę kanałową oraz adapter komunikacji cyfrowej AKC-6000.

Ostatnią prezentację „Oprogramowanie wspomagające POLON Studio" przedstawił inżynier-konstruktor Patryk Sawicki.

Program POLON Studio – Moduł „Konfiguracja i Kompletacja" to nowe narzędzie do konfiguracji, kompletacji i weryfikacji ustawień systemu sygnalizacji pożarowej POLON 6000. Moduł ten jest pierwszym z planowanej serii modułów narzędziowych, przeznaczonych dla profesjonalnych instalatorów oraz osób konfigurujących systemy sygnalizacji pożarowej oparte o rozproszoną centralę POLON 6000.

POLON-ALFA S.A. dziękuje wszystkim zaproszonym Gościom, wykładowcom oraz uczestnikom za przybycie na XXVII Ogólnopolskie Warsztaty SAP '2019 i już dziś zaprasza za rok!

POLON-ALFA

EXTRA LINK

DYNAMITE

AC2100

Jak zwiększyć zasięg sieci wi-fi

Leszek Błaszczyk

Popularność wielofunkcyjnych urządzeń mobilnych w inteligentnych domach i internetowych serwisów, takich jak Netflix czy Spotify, powoduje, że dostęp do sieci wi-fi jest potrzebna w całym domu. Niestety, wiele tradycyjnych routerów bezprzewodowych dostępnych na rynku nie jest w stanie zapewnić zasięgu w całym domu czy biurze

Często nawet wzmacniacze sygnału, zwane potocznie repeaterami, nie są w stanie zagwarantować, że zasięg sieci wi-fi będzie wystarczający. Można również wykorzystać punkt dostępowy, ale emituje on własny identyfikator SSID, więc musimy się ręcznie logować podczas przemieszczania się z jednego miejsca do drugiego. W takiej sytuacji pomocny jest system mesh.

Działanie mesh wi-fi

Najczęściej system mesh jest złożony z trzech lub więcej urządzeń połączonych ze sobą. W skład takiej sieci wchodzi główny router i kilka urządzeń peryferyjnych. Wszystkie elementy łączą się ze sobą drogą bezprzewodową. W związku z tym każdy z nich można umieścić w dowolnym miejscu.

Systemy wi-fi typu mesh kontra wzmacniacze sygnału

W odróżnieniu od wzmacniaczy sygnału, które komunikują się w paśmie 5 GHz i 2,4 GHz bezpośrednio z głównym routerem, elementy systemu mesh nawiązują połączenie nie tylko z głównym routerem, lecz również wzajemnie ze sobą. Każdy węzeł jest punktem przeskoku dla innych węzłów sieci, dlatego węzły umieszczone najdalej od głównego routera także są źródłem silnego sygnału. Można zatem stwierdzić, że bezpośrednia komunikacja odległych węzłów z głównym routerem nie jest konieczna.

Zastosowanie systemu mesh

W miejscach, w których zasięgiem wi-fi chcemy objąć bardzo dużą przestrzeń, takich jak duży dom jednorodzinny lub duże mieszkanie, dobrze sprawdzi się system mesh wi-fi. Znajdzie on zastosowanie również w biurach oraz dużych budynkach firmowych – wszędzie tam, gdzie występują tzw. białe plamy, czyli miejsca, do których sygnał radiowy z głównego routera nie dociera.

Zalety systemu mesh

System mesh jest nowoczesny, niezawodny i wygodny. Umożliwia bezproblemowe korzystanie z Internetu w sieci domowej.

Dzięki niemu w domu lub w siedzibie firmy zasięg może być lepszy, a urządzenia możemy umieścić w dowolnym miejscu. Będziemy w zasięgu sieci we wszystkich pomieszczeniach.

Sygnał jest przekazywany bez żadnych strat. Poszczególne węzły systemu mesh komunikują się zarówno z głównym routerem, jak i wzajemnie ze sobą. Urządzenie wykorzystywane przez użytkownika zmieniającego miejsce pobytu w automatycznie łączy się z najbliższym węzłem, w związku z tym przez cały czas ma dogodne warunki komunikacji.

System mesh działa stabilnie. Węzły komunikują się wzajemnie ze sobą, a nie tylko z głównym routerem. W związku z tym sieć będzie działać poprawnie nawet wówczas, gdy któryś z jej elementów zostanie uszkodzony.

Urządzenia są gotowe do użycia po wyjęciu z opakowania – wystarczy je podłączyć (*plug and play*). Mają domyślnie ustawiony odpowiedni tryb pracy. Użytkownik nie musi zatem posiadać specjalnych umiejętności, by skonfigurować system.

Bez wątpienia największymi zaletami każdego systemu mesh są skalowalność i możliwość łatwej rozbudowy. W celu zwiększenia zasięgu sieci bezprzewodowej w dowolnym miejscu i czasie możemy dołożyć kolejny węzeł. Wszystko to odbywa się bez konieczności konfigurowania czegokolwiek.

Extralink Dynamite

System mesh Extralink Dynamite to bardzo wydajny zestaw trzech urządzeń pracujących w standardzie 802.11ac wave2 AC2100 (główny router i dwa urządzenia peryferyjne). Każde urządzenie wykorzystuje transmisję 4x4 MU-MIMO, przez co sieć bezprzewodowa zyskuje na wydajności. Dynamite został wyposażony w aż trzy chipsety Mediatek, 128 MB pamięci flash i aż 1 Gb pamięci SDRAM, dzięki czemu tworzona jest wydajna sieć o dużej mocy obliczeniowej.

Urządzenia zostały wyposażone w cztery anteny obsługujące pasmo 5 GHz oraz dwie anteny dostosowane do pasma 2,4 GHz. Dzięki takiej liczbie anten Extralink Dynamite zapewni zasięg na powierzchni aż 1000 m^2! Oczywiście Dynamite jest systemem mesh typu plug and play, co umożliwia skonfigurowanie sieci osobom, które nigdy wcześniej tego nie robiły. Dodatkowo ma gigabitowe porty LAN oraz WAN, a także port USB, który umożliwia udostępnianie danych, np. z dysku sieciowego, z wykorzystaniem protokołu FTP albo Samba. Godny uwagi jest też nowoczesny wygląd – Dynamite będzie bardzo dobrze prezentował się w każdym mieszkaniu, apartamencie czy biurze. Zwieńczeniem dzieła jest aplikacja MEshGo!, która umożliwia bardzo szybką i sprawną konfigurację za pomocą smartfonu.

Podsumowanie

Jeżeli szukamy odpowiedniego systemu mesh, powinniśmy wziąć pod uwagę kilka aspektów. Ważny, choć nie najważniejszy, jest wygląd. Powinniśmy zwrócić uwagę na zasięg, obsługiwane standardy wi-fi, np. MU-MIMO, prędkość transmisji bezprzewodowej. Równie istotny jest chipset, pamięć flash, pamięć RAM oraz możliwość korzystania z aplikacji mobilnej. Ważna jest też cena, która powinna być odzwierciedleniem jakości.

W celu zapoznania się z cenami oferowanych przez nas zestawów zapraszam do kontaktu z naszymi sprzedawcami. Na naszym forum można ocenić te produkty. Wasze opinie są dla nas ważne!

Leszek Błaszczyk
www.batna24.com
leszek@batna24.com

EXTRALINK / BATNA24

Przełącz się na Extralink

- zasil swoje kamery i punkty dostępu
- łatwe w zarządzaniu
- zasilanie na odległość do 250m

Porównanie switchy zarządzalnych

Model	VICTOR 24V	VICTOR	ARES	ZEUS	ZEUS V2
Porty	8x GE + 2x SFP	8x GE + 2x SFP	16x GE + 2x SFP	24x GE + 4x SFP	24x GE + 4x SFP+
Porty PoE	8x PoE Pasywne	8x PoE/PoE+	16x PoE/PoE+	24x PoE/PoE+	24x PoE/PoE+
Standard PoE	802.3af	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at
Moc PoE	120W (24V)	150W (48V)	330W (48V)	400W (48V)	440W (48V)
Warstwa	L2	L2	L2	L2	L2 / L3
Tryb AI	✘	✓	✘	✘	✓
Montaż	Desktop	Desktop	1U Rack	1U Rack	1U Rack
Wiatrak	✓	✘	✘	✓	✓

Porównanie switchy niezarządzalnych

Model	EUROS V2	CERES	VIRTUS V2	KRIOS	PERSES	KRATOS
Porty	4x FE + 2x FE	8x FE + 2x FE	16x FE + 1x GE/SFP	4x GE + 2x GE	8x GE + 2x GE	7x GE + 1x GE
Porty PoE	4x PoE/PoE+	8x PoE/PoE+	16x PoE/PoE+	4x PoE/PoE+	8x PoE/PoE+	7x PoE/PoE+
Standard PoE	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at	802.3af / 802.3at
Moc PoE	60W (48V)	96W (48V)	150W (48V)	60W (48V)	96W (48V)	30W/60W/120W (18V/24V/48V/56V)
PoE do 250m	✓	✓	✓	✓	✓	✘
Izolacja portów	✓	✓	✓	✓	✓	✘
Inteligentne zasilanie	✓	✓	✓	✓	✓	✘
Wideo QoS	✓	✓	✓	✓	✓	✘
Montaż	Desktop	Desktop	Desktop / 1U Rack	Desktop	Desktop	Desktop
Wiatrak	✓	✓	✘	✓	✓	✓

Pora na SD WAN

Marek Rekosz

Obecnie każda firma, która ma siedziby w więcej niż dwóch miejscach, musi zadbać o sprawną, nowoczesną i bezpieczną komunikację pracowników i systemów informatycznych

Każdy z operatorów telekomunikacyjnych działających na naszym rynku jest w stanie taką komunikację umożliwić. Może zapewnić łącza internetowe i telekomunikacyjne lub bardziej zaawansowane łącza typu MPLS. Klienci chcą, żeby sieć była coraz lepiej zabezpieczona oraz umożliwiała ustalanie priorytetów dla różnych klas transmisji danych, np. w przypadku aplikacji biznesowych typu ERP, transmisji dźwięku i obrazu czy zwykłego korzystania z przeglądarki internetowej.

Wszystkie te usługi telekomunikacyjne są znane od dawna, a systemy MPLS są dostępne w Polsce od ponad 15 lat. Początkowo sytuacja na rynku była zupełnie inna. Czy możecie sobie wyobrazić symetryczne łącze internetowe typu biznesowego o przepustowości 16 Mb/s za ponad 10 000 zł miesięcznie? Czy pamiętacie, ile czasu czekało się kiedyś na uruchomienie łączy i jak trudno dostępny był światłowód?

Usługi telekomunikacyjne są teraz zupełnie inne, a wymagają tego chociażby nowoczesne aplikacje czy współczesne formy aktywności firm. Oto niektóre aktualne wymagania dotyczące sieci WAN:

- dostęp z każdej lokalizacji do wszystkich kluczowych aplikacji biznesowych, takich jak ERP, CRM itp.,
- połączenie wszystkich oddziałów firm z zachowaniem bardzo wysokiego poziomu bezpieczeństwa,
- dostęp do Internetu z odpowiednimi ograniczeniami dla każdego pracownika,
- bardzo szybki sposób podłączenia nowych oddziałów,

- obniżenie kosztów związanych z wykorzystaniem sieci WAN,
- proste zarządzanie i utrzymanie,
- minimalne zaangażowanie osób z działu IT,
- łatwe i szybkie rekonfiguracje sieci w związku ze zmianą lokalizacji,
- dostęp do aplikacji w chmurze dostępnych przez Internet.

Wydaje się, że nie można wszystkich tych wymagań pogodzić, a jednak czołowi producenci sprzętu sieciowego przychodzą nam z pomocą, proponując nową architekturę sieciową SD WAN.

Geneza SD WAN

Architektura sieciowa SD WAN powstała w USA i od kilku lat jest oferowana przez kilku czołowych producentów urządzeń sieciowych. Można kupić niezbędne składniki i samodzielnie zbudować sieć SD WAN. Na to mogą sobie pozwolić jedynie największe firmy ze względu na koszty i konieczność posiadania dobrych specjalistów. Firmy średnie i małe (pod względem liczby oddziałów) osiągną znacznie więcej korzyści, gdy skorzystają z usługi polegającej na udostępnieniu sieci SD WAN przez operatora, co z pewnością niebawem będzie w coraz większym stopniu dostępne także w Polsce, a nie tylko za oceanem.

Główne założenia dotyczące SD WAN

Twórcy sieci SD WAN wzięli pod uwagę przede wszystkim oczekiwania jakie wymieniłem powyżej, oraz to, co już jest dostępne u operatorów. Istotna była szybka transmisja danych przy cenach znacznie niższych niż za biznesowe łącza. Podstawą SD WAN jest centralny system zarządzania, autoryzacji i bezpieczeństwa z pełną redundancją oraz podłączone do Internetu routery instalowane u klientów. Twórca sieci centralnie konfiguruje ją, ustala priorytety dotyczące transmisji danych dla poszczególnych aplikacji, politykę bezpieczeństwa oraz przypisuje poszczególne urządzenia do określonych lokalizacji. Każdy nowy router instalowany u klienta jest podłączany do zasilania i łącza internetowego. Wykorzystując posiadany trwały i unikalny kod, sam uwierzytelnia się na serwerach producenta i pobiera dostosowane do niego dane konfiguracyjne. Podłączenie sieci w siedzibie klienta jest bardzo proste. Nie ma potrzeby udziału pracowników operatora czy integratora (tzw. *zero touch provisioning*). Ważna jest spójna i jednolita polityka bezpieczeństwa dotycząca wszystkich lokalizacji. Ze względu na podłączenie do Internetu każdy router jest jednocześnie *firewall*em z dodatkowymi zaawansowanymi zabezpieczeniami, które konfigurujemy centralnie.

Niezawodność

Mimo iż w sieciach SD WAN do komunikacji wykorzystywane są głównie łącza internetowe, dzięki ich coraz lepszej jakości (i zaawansowaniu routerów) można uzyskać bardzo dobrą jakość połączenia. Łącza internetowe są dość powszechnie dostępne, a ich przepustowości są coraz większe. Możemy mieć zatem łączność z oddziałami firmy w niższej cenie – w porównaniu z łączami typu MPLS. Połączenie z Internetem można w danym miejscu uzyskiwać drogą światłowodową, dzięki wykorzystaniu łącza typu DSL (w tej samej lokalizacji) oraz dzięki operatorom sieci komórkowych. Istotną właściwością sieci SD WAN i omawianych routerów jest możliwość uzyskania za pomocą jednego urządzenia łączności z Internetem wszystkimi dostępnymi sposobami. Pasma dostępne w poszczególnych kanałach są sumowane, a jakość każdego z nich jest ciągle badana. Dzięki temu można ustawić parametry minimalne wystarczające do transmisji dla poszczególnych aplikacji. Wówczas do transmisji wizyjnych będą wybierane tylko najlepsze łącza. Na rynku oferowanych jest bardzo wiele routerów – od małych urządzeń z portami ethernetowymi 10/100 Mb/s do wielomodułowych urządzeń z wieloma portami ethernetowymi o sumarycznej przepustowości wynoszącej nawet 10 Gb/s, wyposażonych w modemy zapewniające dostęp do sieci komórkowych. Najbardziej istotna jest jednak możliwość ustalania priorytetów dla każdej z aplikacji klienta z osobna. W ten sposób klient uzyskuje najlepszą jakość transmisji danych dla swoich najważniejszych systemów biznesowych. Z pewnością w wielu przypadkach firmy narzekające na wolne działanie systemów typu ERP i CRM po wdrożeniu SD WAN odczują znaczną poprawę.

Bezpieczeństwo

O zabezpieczenia informatyczne sieci SD WAN zadbano ze szczególną starannością. Główne spośród nich:

- autoryzacja (każdy router ma unikalny kod do identyfikacji w sieci, którego nie można zmienić, a jakakolwiek ingerencja sprzętowa powoduje blokadę urządzenia),
- szyfrowanie (to już standard, dlatego transmisja jest szyfrowana za pomocą bardzo złożonych algorytmów),
- każdy router ma zaporę typu *firewall*, a także zabezpieczenie przed złośliwym oprogramowaniem i atakami DDoS,
- centralnie ustalane zasady zabezpieczeń dotyczą wszystkich routerów,
- specjalne połączenia z głównymi dostawcami usług chmurowych, np. Microsoft Office 365, z ciągłym monitorowaniem i utrzymywaniem

najlepszej ścieżki transmisji,
– brak możliwości lokalnej konfiguracji routera jako zabezpieczenie przed zmianami wprowadzanymi przez nieuprawnione osoby.

Szybkość wdrożeń i rekonfiguracji

Firmy są coraz bardziej dynamiczne – otwierają nowe biura, zamykają inne, zanika problem granic między państwami. Takim wyzwaniom jest w stanie sprostać architektura SD WAN. Jedną z jej zalet jest prosta instalacja, którą może przeprowadzić na miejscu ktokolwiek. Wystarczy podłączyć router do zasilania i do Internetu, a jeśli korzystamy z modemów operatorów sieci komórkowych, wystarczy włożyć kartę SIM do każdego z tych modemów. Dzięki temu można znacznie szybciej przeprowadzić instalację w wielu miejscach. W przypadku dużych międzynarodowych projektów zdarza się, że do jednej sieci SD WAN podłączone są urządzenia w 10 tys. miejsc. W przypadku przeniesienia oddziału firmy do innej lokalizacji wystarczy podłączyć router do Internetu w nowym miejscu, a urządzenie samo dokona rekonfiguracji zgodnie z centralnie uzgodnioną metodą autoryzacji. Oczywiście nieuprawnione przeniesienie routera jest natychmiast widoczne w systemach zarządzania i ruch może być blokowany. W sieci SD WAN zarządzanie i wszystkie czynności konfiguracyjne są wykonywane centralnie dla wielu urządzeń jednocześnie, zgodnie z określonymi wzorami.

Prostota

Prostota instalacji i korzystania z sieci SD WAN jest istotna zarówno dla właścicieli i pracowników firm korzystających z usług SD WAN, jak i dla operatorów telekomunikacyjnych i integratorów IT. Trudniej mają ci drudzy, a znacznie łatwiej ci pierwsi. Prawidłowa konfiguracja systemów zarządzania siecią SD WAN w chmurze, określenie zasad dotyczących bezpieczeństwa i sposobów regulacji przepływu danych z różnych aplikacji itp. wymaga zaawansowanej wiedzy i dlatego jest to usługa dostępna dla operatorów posiadających odpowiednią kadrę. W przypadku modelu usługowego w ramach usługi udostępnienia sieci SD WAN klient dostaje panel do podglądu, który umożliwia sprawdzanie działania całej sieci, i urządzenia końcowe. Nie musi zatrudniać własnych specjalistów telekomunikacyjnych oraz kupować osobnych urządzeń i licencji w celu zapewnienia bezpieczeństwa, np. zapór typu *firewall*, a także własnych routerów.

Oszczędności

Oprócz lepszej jakości i szybkości działania sieci SD WAN, które oczywiście przekładają się na lepszą produktywność firm, nie do pominięcia są znaczne oszczędności, jakie można uzyskać (biorę tu pod uwagę model usługowy dla średnich i małych firm). Niższe są koszty łączy. Koszt urządzeń dostarczanych przez operatora jest wliczony w abonament. Nie jest konieczne posiadanie jednego głównego łącza internetowego. Każdy router jest też zaporą typu *firewall*. Nie są potrzebne dodatkowe zabezpieczenia sprzętowe oddziałów. Utrzymanie sieci jest znacznie prostsze, więc informatycy mają czas na inne zadania.

Podsumowanie

Pewnie zastanawiają się Państwo, czy sieci SD WAN rzeczywiście się rozwiną i utrzymają na rynku. Gdy po raz pierwszy o nich usłyszałem, bardzo dokładnie zapoznałem się z podejściem producentów do tego tematu, z problemami, jakie mają operatorzy i klienci, z założeniami biznesowymi i strategiami firm. To, czego się dowiedziałem, całkowicie utwierdziło mnie w przekonaniu, że sieci SD WAN są potrzebne operatorom, integratorom i klientom biznesowym. Potwierdzają to coraz bardziej widoczne trendy rynkowe. Internet staje się medium transmisyjnym o coraz lepszej jakości. Routery są coraz bardziej zaawansowane. W związku z tym możliwe są zaawansowane zabezpieczenia, szyfrowanie szybkich łączy itp. Klienci chcą korzystać z aplikacji chmurowych. Prawie każdy pracownik musi mieć dostęp do Internetu, a jednocześnie trzeba zachować wysoki poziom bezpieczeństwa sieci biurowych. Dynamika zmian w biznesie stwarza coraz większy problem z akceptacją długoterminowych umów dotyczących korzystania z sieci WAN w wielu lokalizacjach. Usługi i sieci SD WAN bardzo dobrze wykorzystują możliwości techniczne urządzeń, oprogramowania i operatorów, więc skorzystanie z nich może być rozwiązaniem problemów wielu firm. Jeżeli przy tym koszty będą mniejsze niż obecnie, powszechne udostępnienie ich w Polsce będzie tylko kwestią czasu.

Marek Rekosz

OGÓLNOPOLSKIE STOWARZYSZENIE KONSULTANTÓW ZAMÓWIEŃ PUBLICZNYCH

OSKZP

20 lat

OGÓLNOPOLSKIE STOWARZYSZENIE KONSULTANTÓW ZAMÓWIEŃ PUBLICZNYCH

Ogólnopolskie Stowarzyszenie Konsultantów Zamówień Publicznych działa od 1998 r. i jest najdłużej funkcjonującym w Polsce stowarzyszeniem, zajmującym się tematyką zamówień publicznych. Aktualnie zrzesza ok. 140 członków – specjalistów w wielu dziedzinach, praktyków prawa zamówień publicznych oraz byłych arbitrów i trenerów z listy Prezesa Urzędu Zamówień Publicznych.

Głównym celem założenia i funkcjonowania Stowarzyszenia jest upowszechnianie zagadnień z zakresu zamówień publicznych wśród zamawiających i wykonawców .

doskonalenie funkcjonowania systemu zamówień publicznych, wymiana doświadczeń oraz doskonalenie umiejętności i poszerzanie wiedzy wśród członków Stowarzyszenia, współpraca z organizacjami krajowymi i zagranicznymi o podobnych celach działania, inspirowanie oraz wspieranie działań zmierzających do podnoszenia etyki zawodowej osób zajmujących się zamówieniami publicznymi oraz integrowanie środowiska osób zajmujących się zamówieniami publicznymi.

Cele Stowarzyszenia realizowane są w szczególności poprzez:

1. organizowanie lub współorganizowanie warsztatów, szkoleń, seminariów lub konferencji dla swoich członków lub osób zajmujących się zamówieniami publicznymi,
2. współpracę z wydawnictwami i mediami,
3. przygotowanie i upowszechnianie opinii do projektów aktów prawnych, dotyczących zamówień publicznych,
4. organizowanie spotkań z przedstawicielami administracji publicznej i innymi instytucjami,
5. przedstawianie właściwym organom postulatów i opinii w sprawach związanych z celami oraz z działalnością Stowarzyszenia i jego członków,
6. propagowanie zasad etyki zawodowej i dbanie o ich przestrzeganie.

Potwierdzeniem pozycji OSKZP na rynku podmiotów zajmujących się zamówieniami publicznymi jest fakt, że jako jedna z 8 organizacji pozarządowych jest imiennie zapraszana przez Prezesa Urzędu Zamówień Publicznych do zgłaszania uwag i propozycji do projektów aktów wykonawczych do prawa zamówień publicznych, przygotowywanych przez stronę rządową.

Dwóch członków Stowarzyszenia zostało ponadto powołanych przez Ministra Przedsiębiorczości i Technologii w skład nowej Rady Zamówień Publicznych.

Stowarzyszenie współuczestniczyło lub nadal bierze udział w projektach finansowanych ze środków unijnych:

- PHARE 2002 – projekt pn. Zwiększanie znajomości procedur zamówień - projekt zrealizowany przez Urząd Zamówień Publicznych, obejmujący 187 dwudniowych szkoleń dla około 5400 uczestników, zakończony w 2005 r. - członkowie Stowarzyszenia byli w projekcie wykładowcami,
- PHARE 2003 – projekt pn. Doskonalenie praktyki i mechanizmów kontrolnych dotyczących zamówień publicznych - ujednolicenie i popularyzacja dobrych praktyk związanych z udzielaniem zamówień publicznych – szczególnie mechanizmów kontroli. Członkowie Stowarzyszenia byli w projekcie współautorami publikacji pt. „Praktyczny przewodnik dla korzystających z wzorcowej dokumentacji przetargowej i wzorów umów w sprawach zamówień publicznych" oraz „Analiza wyroków sądów okręgowych oraz analiza orzeczeń zespołów arbitrów wydanych na podstawie ustawy Prawo Zamówień Publicznych",
- Projekt KIGNET - izbowy system wsparcia konkurencyjności polskich przedsiębiorstw. Projekt realizowany był wspólnie przez organizacje członkowskie oraz Krajową Izbę Gospodarczą, w ramach Sektorowego Programu Operacyjnego Wzrost Konkurencyjności Przedsiębiorstw, lata 2004-2006, Priorytet 1 Rozwój przedsiębiorczości i wzrost innowacyjności poprzez wzmocnienie instytucji otoczenia biznesu, Działanie 1.1 Wzmocnienie instytucji wspierających działalność przedsiębiorstw, Poddziałanie 1.1.2 Wsparcie instytucji otoczenia biznesu oraz sieci instytucji otoczenia biznesu. W ramach projektu, Stowarzyszenie przeprowadziło cykl szkoleń doskonalących wiedzę doradców i trenerów zamówień publicznych oraz wydało Poradnik dla Wykonawców Zamówienia publiczne. Po zakończeniu projektu (wrzesień 2007 r.) 56 osób - członków Stowarzyszenia zostało wpisanych na listę ekspertów, doradców i wykładowców zamówień publicznych.
- Projekt pn. Dobre praktyki z zakresu działań antykorupcyjnych - Stowarzyszenie było podwykonawcą Krajowej Izby Gospodarczej. Celem Projektu było wspomaganie społecznych inicjatyw antykorupcyjnych poprzez promocję dobrych praktyk, konsekwencją czego było podnoszenie świadomości społecznej w zakresie działań antykorupcyjnych.

Ogólnopolskie Stowarzyszenie Konsultantów Zamówień Publicznych
e-mail: biuro@oskzp.pl
http://www.oskzp.pl/

Szanse i wyzwania dla branży ochrony w 2020 roku

Łukasz Koch

Ochrona to dość specyficzny rodzaj działalności. Z jednej strony firmy ochrony są odpowiedzialne za bezpieczeństwo swoich klientów i ich mienie, przez co uzupełniają i wspierają służby publiczne, a z drugiej zawód pracownika ochrony nie cieszy się uznaniem społecznym. Wynika to między innymi z przeświadczenia, że może nim zostać każdy. Te czasy jednak powoli mijają

Za pracownikiem ochrony coraz częściej stoją nowoczesne rozwiązania techniczne, zintegrowane systemy zabezpieczeń, które wymagają obsługi specjalistycznych programów, umiejętności analizy sytuacji i podejmowania właściwych działań. Niektórzy uważają, że nie warto płacić za coś, czego nie widać. Faktycznie – w związku z cyfryzacją, automatyzacją i możliwością zdalnego nadzoru pracownicy ochrony nie są już tak widoczni w obiektach. Świadczy to jednak o nowoczesnych narzędziach pracy i wysokiej jakości usług, a nie o braku konieczności ochrony lub możliwości nadmiernej redukcji kosztów. W opozycji do oczekiwań klientów obniżenia kosztów stoją zmiany legislacyjne podnoszące wysokość minimalnego wynagrodzenia i zapowiadające oskładkowanie wszystkich zleceń. Dużym problemem dla branży jest brak pracowników. Nadchodzący rok 2020 będzie pełen wyzwań w związku ze zmianami legislacyjnymi, wdrażaniem nowych rozwiązań dla klientów, a także walką o pracowników i pozytywny wizerunek branży.

Zmiany legislacyjne

Ceny usług związanych z ochroną fizyczną od wielu lat kształtuje wysokość minimalnego wynagrodzenia. Składa się na to duża liczba firm na rynku, ostra konkurencja cenowa, presja klientów oraz wpływ sektora zamówień publicznych, gdzie – mimo zmian w ustawie – w dalszym ciągu podstawowym kryterium wyboru oferenta jest cena. Ponadto część firm ochrony, szukając szansy na redukcję kosztów, korzysta z umów cywilnych, mimo że w wielu przypadkach charakter wykonywanej pracy nakazuje stosowanie umowy o pracę.

W 2020 r. wysokość minimalnego wynagrodzenia za pracę będzie wynosić 2600 zł brutto, a wysokość minimalnej stawki godzinowej dla umów-zleceń 17 zł brutto (zgodnie z rozporządzeniem

Rady Ministrów z 18 września br.). Jest to wzrost minimalnego wynagrodzenia o 15,6%, odpowiadający kwocie 350 zł, co stanowi największy wzrost minimalnego wynagrodzenia od ponad dziesięciu lat. Ostatnia tak duża zmiana miała miejsce w roku 2007 i wynosiła ponad 20%.

Kalkulacje budżetów na usługi ochrony w 2020 r. muszą uwzględnić również uruchomienie pracowniczych planów kapitałowych (PPK) skutkujących wzrostem obciążeń po stronie pracodawcy o 1,5% wynagrodzenia pracownika brutto. Pracownicy są na mocy przepisów prawa zapisywani do PPK i samodzielnie decydują o ewentualnej rezygnacji, dlatego obecnie trudno dokładnie oszacować koszty związane z tym programem.

Bardzo prawdopodobne jest również pełne oskładkowanie zleceń zapowiedziane w przyjętym przez Radę Ministrów Wieloletnim Planie Finansowym Państwa na lata 2019–2022. W dniu 24 września br. Rada Ministrów przyjęła projekt budżetu państwa na rok 2020, w którym uwzględnione zostały przychody z pełnego oskładkowania umów-zleceń.

Koszty wynagrodzeń stanowią 75% – 80% kosztów realizacji usług. Wprowadzona zmiana wysokości minimalnego wynagrodzenia oraz program PPK powoduje wzrost tych kosztów o 17%, co powinno znaleźć odzwierciedlenie we wzroście stawek za usługi. W przypadku firm ochrony, które do tej pory stosowały głównie umowy-zlecenia, wzrost stawek będzie wymagany na jeszcze wyższym poziomie, tj. około 30% lub więcej. Wynika to z konieczności uwzględnienia w kalkulacji ceny usługi wzrostu stawek minimalnych oraz oskładkowania wszystkich umów-zleceń.

Tak duże zmiany kosztów płacowych stanowią wyzwanie zarówno dla firm ochrony, jak i dla klientów. Część firm obawia się wielkości podwyżek, gdyż będą one dla nich zbyt dużym obciążeniem finansowym. Inne dostrzegają sposobność na wyrównanie szans i uczciwą konkurencję. Pracownicy mają nadzieję na poprawę warunków zatrudnienia i wyższe zarobki przy mniejszych obciążeniach czasowych.

Braki kadrowe i wizerunek branży

Problemy z pozyskiwaniem pracowników w branży ochrony występują nie tylko w Polsce, lecz w całej Europie. Według Eurostatu w sierpniu 2019 r. poziom bezrobocia w Czechach wynosił 2%, w Niemczech 3,1%, w Polsce 3,3%, na Węgrzech 3,4%, a w Holandii 3,5%. Brak rąk do pracy jest szczególnie odczuwalny w usługach i w handlu. Firmy prześcigają się w budowaniu atrakcyjnych ofert pracy, walcząc o kandydatów, tymczasem sektor ochrony jest pod tym względem bierny. W dużych firmach ochrony brakuje od 150 do 400 albo więcej pracowników, rotacja roczna jest na poziomie 60% – 80%, a w obiektach handlowych

jeszcze wyższa. Nadal dominują formy zatrudnienia zniechęcające kandydatów do podjęcia pracy (zlecenie, nieregularne wypłaty) i bardzo trudno jest przyciągnąć i utrzymać pracowników w wieku do 25 lat. Praca w ochronie nie jest dla nich ani ciekawa, ani atrakcyjna finansowo. W konsekwencji szkoły zawodowe zamykają kierunki kształcące pracowników ochrony ze względu na brak zainteresowania. Na dziesięć szkół losowo wybranych w aglomeracji śląskiej tylko trzy zdecydowały się na nabór na kierunek związany z ochroną, a finalnie zajęcia nie zostały rozpoczęte ze względu na brak kandydatów.

Wiele wskazuje jednak na to, że ta sytuacja powinna niedługo ulec zmianie. W związku z wdrażaniem nowych technologii, zintegrowanych systemów zabezpieczeń, zdalnych form ochrony i analizy treści obrazu branża będzie potrzebować osób o wyższych kwalifikacjach. Na razie jednak dominuje zatrudnienie ludzi w wieku powyżej 40 lat, co stanowi ok. 60% lub więcej ogółu zatrudnionych**. Często są to osoby o niskich kwalifikacjach i wykształceniu zasadniczym, które nie mogą znaleźć pracy w innych sektorach rynku. W wielu przypadkach pracują z zaangażowaniem i wykonują dobrze swoją pracę, jednak liczba miejsc pracy dostępnych dla osób o takim profilu zawodowym będzie systematycznie malała. Liczba kwalifikowanych pracowników ochrony gotowych pracować w swoim zawodzie systematycznie spada, ponieważ wynagrodzenia pracowników kwalifikowanych i bez kwalifikacji często są na tym samym poziomie.

Problem zatrudnienia, z jakim zmagają się firmy ochrony, jest ściśle powiązany z wizerunkiem w całej branży, na który składa się wiele elementów. Nieregularne wypłaty, niskie wynagrodzenia, różne formy zatrudnienia, brak szkoleń, szans rozwoju oraz ścieżek kariery to niestety problemy wielu firm. Wizerunek branży jest niekorzystny również w Internecie, np. w mediach społecznościowych, co również zniechęca do podjęcia pracy w ochronie.

Firmy ochrony najczęściej nie podejmują żadnych działań mających na celu korzystne zaprezentowanie się w Internecie, co szczególnie dla młodych ludzi jest często czynnikiem decydującym o wyborze pracy. Rok 2020 może być dla firm ochrony czasem przełomowym. Zmiany legislacyjne i podwyższenie wynagrodzeń to okazja do przyciągnięcia kandydatów do pracy. Jednak pozyskanie osób już zatrudnionych będzie wymagało podjęcia nowych działań. Walka z negatywnym wizerunkiem to zadanie przewidziane na kilka lat. Zmiany należy zacząć wprowadzać wewnątrz firm już dziś i eliminować powody negatywnych ocen.

Klienci

Dla klientów wzrost kosztów zatrudnienia to również poważne wyzwanie. W niektórych branżach, np. motoryzacyjnej i budowlanej, odczuwalne są symptomy zbliżającej się recesji, które skłaniają raczej do oszczędności i ograniczenia wydatków niż do inwestowania w usługi związane z ochroną. Z tego względu skłonność klientów do zaakceptowania podwyżki stawek za ochronę na poziomie 17% może być trudna, a na poziomie 30% wręcz niemożliwa. Klienci będą z pewnością porównywać oferty, kierując zapytania do innych firm, co może skutkować utratą kontraktów. Niestety niektórzy klienci nadal otwarcie pytają o możliwość zawarcia z pracownikami ochrony umów cywilnych. Takie praktyki budzą wiele kontrowersji.

Negocjacje podwyżek z klientami będą trudne i być może przyczynią się do ograniczonego korzystania z ochrony fizycznej i zwiększenia zainteresowania usługami zdalnymi, opartymi na rozwiązaniach technicznych, w tym również mobilnych. Po zmianie cen klienci będą zwracali jeszcze większą uwagę na jakość świadczonych usług, wskaźniki efektywności, gwarancje, wpływ ochrony na rozwój ich biznesu i wartości dodatkowe. Szansą dla firm ochrony może być zatem otwartość na zmiany i wdrażanie nowych rozwiązań, które umożliwią obniżenie kosztów w roku 2020 i latach następnych.

Znacznie większym wzywaniem będzie jednak rynek zamówień publicznych, gdzie nadal jedynym kryterium wyboru jest cena.

Scenariusze na 2020 rok

Tak duża skala zmian, silnie oddziaływująca na koszty ponoszone przez pracodawców, oraz niekorzystne uwarunkowania otoczenia rynkowego będą wymagać innego niż dotychczas podejścia do oferowanych usług, pracowników i klientów. Można wymienić cztery podstawowe, potencjalne scenariusze działania, jakie mogą w tej sytuacji być brane pod uwagę:

Scenariusz 1. – bierna postawa i działanie oparte na dotychczasowych zasadach, bez dokonywania zmian w sposobie funkcjonowania firmy, zarówno wobec pracowników jak i klientów. W tym przypadku będzie bardzo trudno przetrwać i utrzymać się na rynku. Koszty będą rosły szybciej niż potencjalne przychody.

Scenariusz 2. – rezygnacja z działalności z powodu nowych uwarunkowań, próba sprzedaży lub likwidacji firmy albo zmiana profilu działalności. Sprzedaż może być trudna ze względu na niską rentowność kontraktów i dotychczas stosowane formy zatrudnienia, które w nowych okolicznościach rynkowych będą decydować o wartości i potencjale danej firmy.

Scenariusz 3. – dotychczasowa działalność zostanie trochę zmodyfikowana, ale sposób działania nie ulegnie zmianie i nadal będzie bazować na nietransparentnych lub ryzykownych rozwiązaniach, rozbudowanej administracji oraz trikach w obszarze zatrudniania skutkujących narażeniem na interwencje zewnętrznych instytucji kontrolnych oraz rosnącą skalę sporów pracowniczych.

Scenariusz 4. – zmiana modelu biznesowego, transparentne działania wobec klientów i pracowników, poszukiwanie nowych rozwiązań dla klientów, wsparcie ochrony fizycznej atrakcyjnymi cenowo i efektywnymi rozwiązaniami technicznymi.

Osobiście jestem zwolennikiem czwartego scenariusza, aczkolwiek wymaga on aktywności i inicjatywy. Otoczenie administracyjne, rynek pracy i możliwości klientów zdecydowanie potrzebują nowego podejścia. Najbardziej pożądane wydają się rozwiązania, które umożliwią dalszą współpracę z klientami dzięki aktywnej modyfikacji lub wręcz transformacji dotychczasowego systemu ochrony. W tym celu wskazane jest korzystanie w większym zakresie z rozwiązań technicznych umożliwiających redukcję liczby roboczogodzin. Zaoszczędzone w ten sposób środki warto przeznaczać na rozbudowywanie systemu ochrony i podwyższenie wynagrodzeń pracowników. Niezbędne jest również odejście od kalkulacji opartej na minimalnych stawkach za roboczogodziny. Trzeba konstruować rozwiązania bazujące na budżetach, aby zapewnić klientowi większą stabilność i przewidywalność kosztów w odpowiednio długim okresie, a także zaoferować wykwalifikowanym pracownikom płacę znacznie wyższą od minimalnej.

W najbliższym czasie niekoniecznie wygra ten, kto wynegocjuje najwyższą stawkę u klienta, ale ten, kto zmieni swój sposób działania i znajdzie rozwiązania korzystne dla obu stron. Powinno to także umożliwiać pozyskiwanie lepszych pracowników oraz podnosić jakość i skuteczność oferowanych usług. Rok 2020 może wyrównać szanse małych, średnich i dużych firm. Wiele zależy od inwencji, pomysłów i determinacji w ich realizacji. W tym zakresie życzę powodzenia firmom ochrony, ich obecnym i przyszłym pracownikom oraz klientom.

Łukasz Koch
członek zarządu, dyrektor ds. HR,
Securitas Polska
członek zarządu
Polskiego Związku Pracodawców Ochrona

* W momencie pisania tego tekstu nie były znane finalne decyzje dotyczące oskładkowania zleceń.
** Dane o charakterze szacunkowym, wynikające z rozmów z firmami z branży ochrony.

Rozmieszczanie czujek pożarowych na płaskim stropie

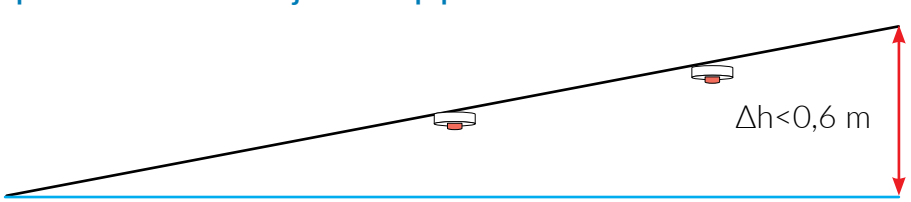
Część 1

Jerzy Ciszewski

Rozmieszczanie czujek pożarowych na płaskim stropie wydaje się zajęciem prostym. Dokonuje się go w większości projektów systemów sygnalizacji pożarowej

Projektant instalacji sygnalizacji pożarowej powinien nie tylko znać zasady rozmieszczania czujek, ale także rozumieć, dlaczego te zasady są takie, jakie są. I najważniejsze – powinien zdawać sobie sprawę z pewnych uproszczeń tych zasad, które czasami niemal ocierają się o lekceważenie zasad fizyki. Niniejszy artykuł zawiera przegląd (na pewno niepełny) zasad rozmieszczania czujek pożarowych na płaskich stropach.

Kiedy strop można traktować jako strop płaski?

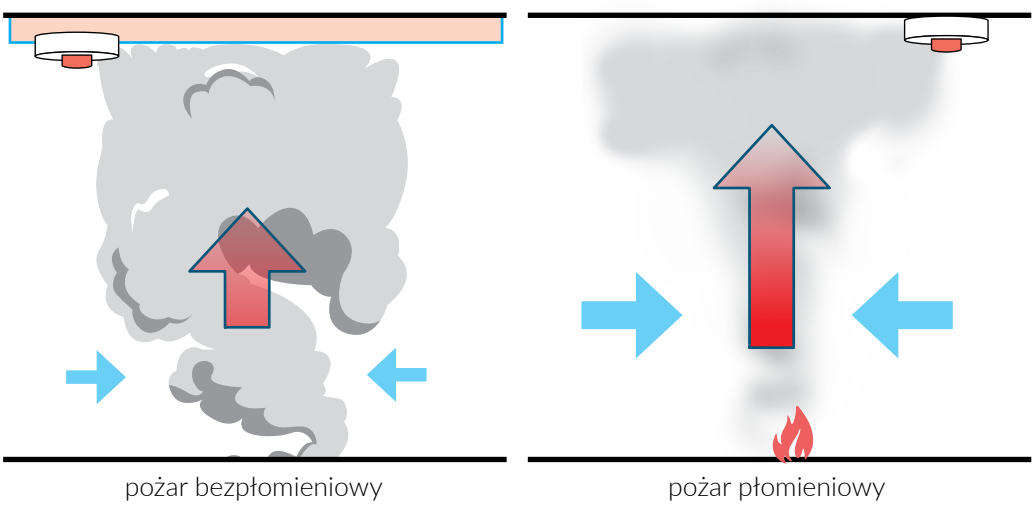


Rys. 1. Kryterium „płaskości" stropu

W specyfikacji CEN TS54-14:2018 podano następującą informację:
„Jeśli różnica wysokości między dolną a górną częścią stropu ukośnego jest mniejsza niż 600 mm, strop może być traktowany tak, jakby był płaski. Dotyczy przypadku, gdy stosowane są czujki dymu. Dla czujek ciepła należy przyjąć odległość 150 mm".

Zasięg czujki

Przemieszczanie się dymu ku górze wynika ze zjawiska wyporu. Ciepło wytworzone w procesie spalania podgrzewa powietrze, które – jako mniej gęste od otaczającego je powietrza – wraz z porwanymi drobinami dymu przemieszcza się ku górze, wypychane przez napierające z boku chłodne powietrze. Dym przemieszcza się do góry w formie pióropusza, którego kształt jest zależny od ilości ciepła wytworzonego w czasie pożaru. Jest to pokazane na rysunku 2.



Rys. 2. Sposób przemieszczania się dymu w zależności od rodzaju pożaru

Wraz ze wzrostem wysokości stężenie dymu oraz jego temperatura na poszczególnych poziomach w pióropuszu maleje. Jednocześnie, po dotarciu do stropu, dym, rozprzestrzeniając się na wszystkie strony, ma coraz mniejszą gęstość oraz temperaturę.

W praktyce procedura rozmieszczania czujek pożarowych sprowadza się do określenia odległości od osi pożaru, przy której koncentracja dymu jest jeszcze dostatecznie wysoka, aby pobudzić układ pomiarowy czujki dymu, lub temperatura jest dostatecznie wysoka, aby uruchomić czujkę ciepła. W wytycznych dotyczących projektowania podano w formie tabelarycznej odpowiednie wartości tej odległości, określając ją jako zasięg czujki lub promień działania czujki.

Przy określaniu promienia działania czujki i związanej z nim maksymalnej powierzchni dozorowania oraz maksymalnej wysokości instalowania bierze się pod uwagę różne czynniki:

1. Początkowy charakter rozwoju pożaru. Nie zawsze można go jednoznacznie określić. Jest on zależny między innymi od rodzaju i ilości paliwa, sposobu inicjacji itp.
2. W przypadku pożaru płomieniowego gorące powietrze bardzo szybko wynosi dym na wysokość 12–16 m, a pióropusz dymu tworzy stożek o małym kącie rozwarcia.
3. Szybkie przemieszczanie się drobin dymu ku górze ogranicza w wysokim stopniu zjawisko tworzenia się agregatów, czyli dużych cząstek.
4. W przypadku pożaru bezpłomieniowego dym nie tylko przemieszcza się ku górze, ale również silnie rozprzestrzenia się na boki. Ponieważ nie ma silnej konwekcji, dym nie jest w stanie dotrzeć na duże wysokości.
5. Ze względu na powolny proces pożarowy drobiny dymu przez długi czas przebywają blisko siebie. Umożliwia to tworzenie się agregatów, a więc następuje zwiększenie się wielkości drobin aerozolu.

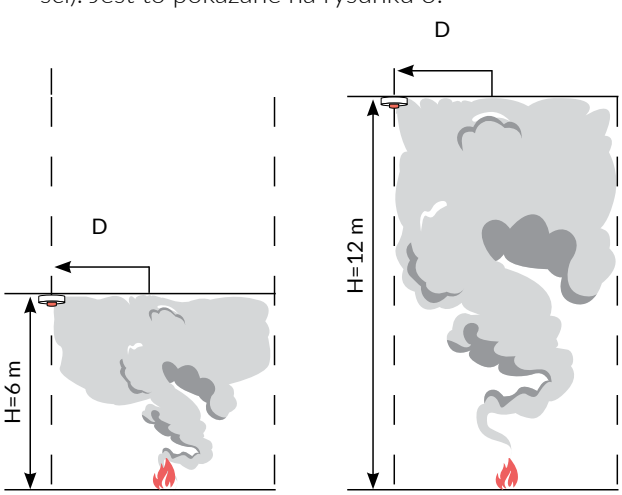
Chcąc uprościć procedurę wyboru wielkości nadzorowanej przez czujkę dymu przestrzeni, bez względu na charakter spodziewanego pożaru, powinniśmy brać pod uwagę najgorsze warianty. Zasięg punktowej czujki dymu i wynikająca z niego powierzchnia dozorowania powinny być w takim razie ograniczone, jak w przypadku pożaru płomieniowego, i wynikać bezpośrednio z faktu przemieszczania się dymu po stropie. Maksymal-

na wysokość, na jakiej powinno się zainstalować punktową czujkę dymu, powinna być ograniczona, jak w przypadku pożaru bezpłomieniowego.

Podstawowe założenia przyjęte w metodykach projektowania rozmieszczenia czujek

Zasada stałej wartości zasięgu czujki w funkcji wysokości instalowania

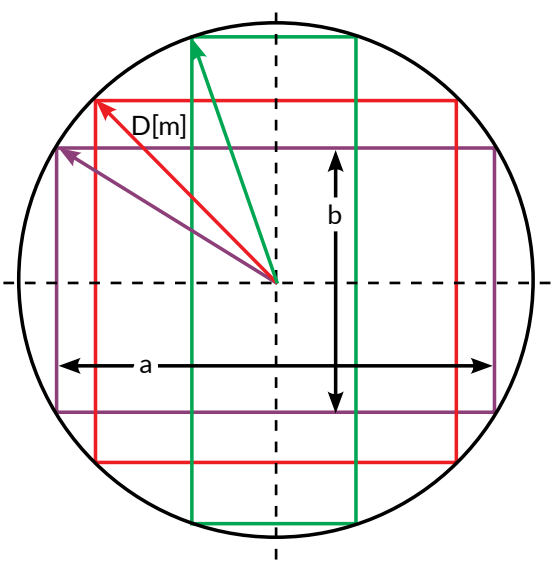
Dla uproszczenia procesu projektowania przyjęto zasadę, że zasięg czujki mierzony od osi pożaru do miejsca zainstalowania czujki jest stały i nie zależy od wysokości, na jakiej jest zainstalowana (wysokości stropu). Przyjmuje się takie założenie, jeżeli ta wysokość nie przekracza ok. 12 m. Można więc przyjąć na przykład, że na wysokościach 6 m oraz 12 m, w odległości D od osi pożaru stężenie dymu jest takie samo (na takie stężenie reaguje czujka dymu zainstalowana w tej odległości). Jest to pokazane na rysunku 3.



Rys. 3. Zasada stałej wartości zasięgu D czujki w funkcji wysokości instalowania H. Na rysunku nie zaznaczono poduszki powietrznej

Powyższą zasadę przyjęto, opracowując wytyczne dotyczące projektowania, zawarte między innymi w:

- specyfikacji technicznej PKN-CEN/TS 54-14:2004 (a także w późniejszych wersjach) opracowanej przez CEN oraz wydanej w Polsce przez PKN,
- zaleceniach SITP WP-02:2010,
- brytyjskiej normie w wersjach z lat 2002–2013 (od BS 5839-1:2002 *Fire detection and fire alarm systems for buildings. Code of practice for system design, installation, commissioning and maintenance* do BS 5839-1:2013 *Fire detection and fire alarm systems for buildings. Code of practice for design, installation, commissioning and maintenance of systems in non-domestic premises*),
- *NFPA 72: National Fire Alarm and Signaling Code* – zasada obowiązuje do pewnej wysokości (i dotyczy czujek ciepła).



Rys. 4. Powierzchnie dozorowania czujki wpisane w okrąg o promieniu D. Strop płaski

Zasada stałego zasięgu umożliwia nadzorowanie przez pojedynczą czujkę przestrzeni, której rzut na strop będzie zawarty wewnątrz okręgu o promieniu D. W rzeczywistości nadzorowana powierzchnia ma w większości przypadków kształt prostokątny albo – niezwykle rzadko – kwadratowy.

Optymalnym sposobem rozmieszczania czujek jest podział kwadratowy, co widać na rysunku 4. W takim przypadku powierzchnia nadzorowana przez czujkę jest największa (oczywiście nie uwzględnia się tu możliwości nadzorowania rotundy).

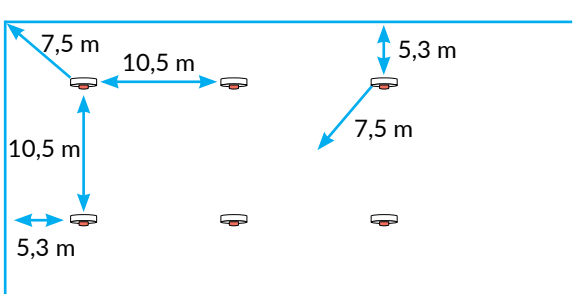
Wartości zasięgów D (promieni działania, wysokości instalowania) są wybrane zgodnie z wytycznymi SITP WP-02:2010.

rodzaj czujki	wysokość pomieszczenia H [m]					
	≤ 4,5	> 4,5 ≤ 6	> 6 ≤ 8	> 8 ≤ 11	> 11 ≤ 25	> 25
	promień działania D [m]					
czujki ciepła:						
klasa 1; A1	5	5	5	NN	-	-
klasa 2; A2, B..G	5	5	NN	-	-	-
klasa 3	5	NN	-	-	-	-
czujki dymu:						
punktowe	7,5	7,5	7,5	7,5	NN	-
liniowe	6,0	6,0	6,5	6,5	6,5*	-
czujki wielodetektorowe:						
dymu i ciepła (A1)	5,0	5,0	5,0	NN	-	-
dymu i ciepła (A1) i CO	5,0	5,0	5,0	NN	-	-
dymu i/lub CO	7,5	7,5	7,5	7,5	-	-
objaśnienia:						
-	nieprzydatna do stosowania w przypadku danej wysokości pomieszczenia					
NN	normalnie nieprzydatna, lecz może być zastosowana w rozwiązaniach specjalnych					
*	w połowie wysokości pomieszczenia wymagany jest drugi poziom czujek					

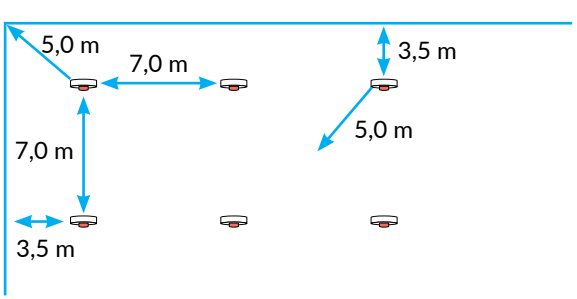
Tab. 1.

W przypadku podziału kwadratowego zalecane maksymalne odległości dla czujek dymu są pokazane na rysunku 5.

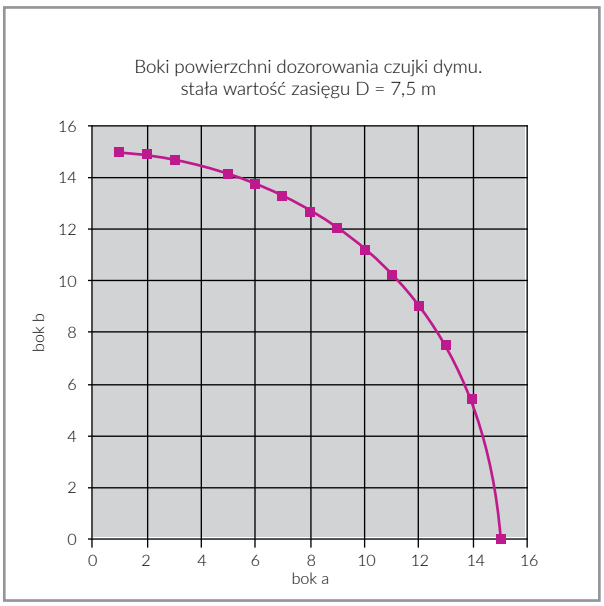
Na rysunku 6 podano te odległości dla czujek ciepła.



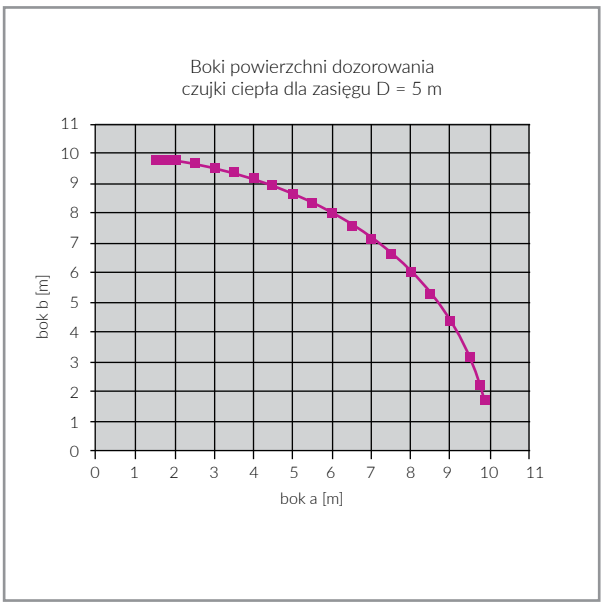
Rys. 5. Rozmieszczenie czujek dymu. Przypadek graniczny. Podział kwadratowy



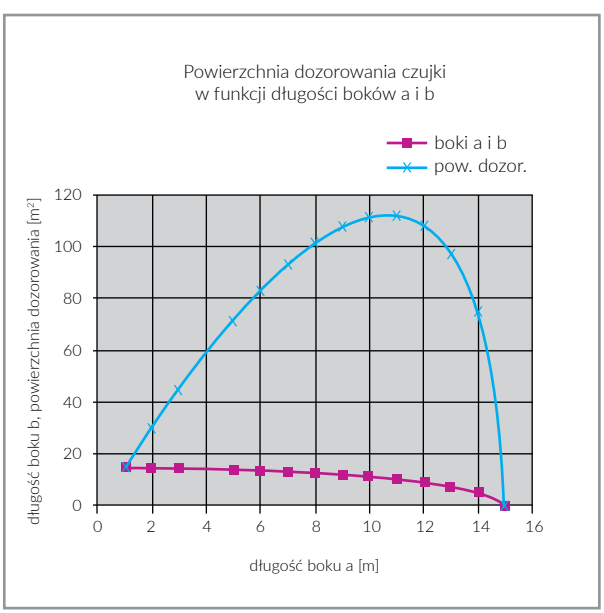
Rys. 6. Rozmieszczenie czujek ciepła. Przypadek graniczny. Podział kwadratowy



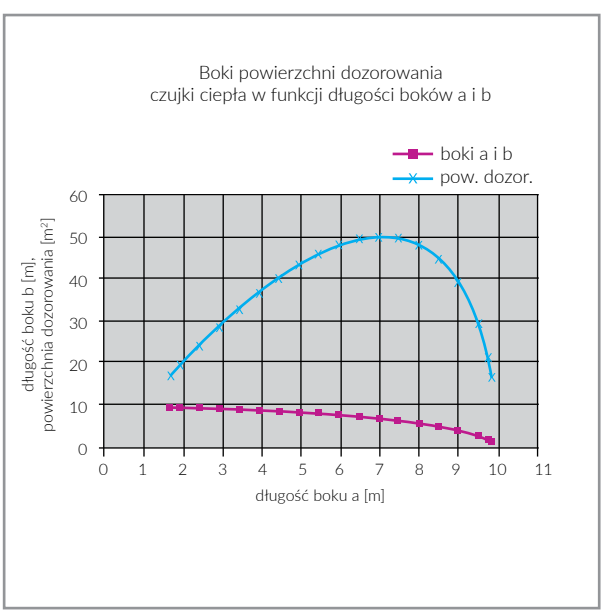
Rys. 7. Dopuszczalna zmienność boków powierzchni dozorowej czujki dymu



Rys. 9. Dopuszczalna zmienność boków powierzchni dozorowej czujki ciepła



Rys. 8. Zależność powierzchni dozorowej czujki od długości boków



Rys. 10. Zależność powierzchni dozorowej czujki ciepła od długości boków

Na rysunku 8 widać wyraźnie, że odejście od kwadratowego podziału powoduje gwałtowne zmniejszenie powierzchni dozorowania czujki dymu. Na kolejnych rysunkach pokazano analogiczne zależności dotyczące punktowych czujek ciepła.

Maksymalne wysokości instalowania (zgodnie z CEN/TS54-14:2018)

wysokość pomieszczenia [m]	czujka dymu EN 54-7	liniowa czujka dymu EN 54-12	zasysająca czujka dymu EN 54-20 (klasy A, B, C)	punktowa czujka ciepła EN 54-5 (klasy A1, A2, B, C, D, E, F, G[b a])	liniowa czujka ciepła EN 54-22 (klasy A1, A2)	czujka płomieni EN54-10 (klasy 1,2,3)
do 45		e, f	> 15 otworów, klasa B[f]			
do 25		d, f	> 15 otworów, klasa C[f]			
do 16			> 5 otworów, klasa C[f]			
do 12						
do 9					A1	
do 7,5				A1	A2	
do 6				A1, A2	A2	
	nieodpowiednia					
	odpowiednia albo nieodpowiednia w zależności od zastosowania i warunków środowiskowych, np. odpowiednia w przypadku szybkiego rozprzestrzeniania się dymu i ognia					
	odpowiednia					
a	także czujki klasy R lub S					
b	klasy B, C, D, E, F ,G – odpowiednie tylko do zabezpieczania obiektów					
c	w zależności od klasy zadziałania oraz od rozmieszczenia czujek					
d	akceptowane w przypadku potwierdzenia wydajności					
e	zalecana wartość czułości – 35% tłumienia lub mniejsza					
f	wymagane potwierdzenie za pomocą pożarów testowych					

Tab. 2. Maksymalne wysokości instalowania zgodnie z CEN/TS54-14:2018 (punkt 6.5.1)

Uwagi:

1. Z danych podanych w tabeli 2 wynika możliwość nadzorowania punktowymi czujkami dymu pomieszczeń o wysokościach przekraczających 12 m w przypadku, w którym scenariusz pożarowy zawiera informacje dotyczące możliwości wystąpienia tylko pożaru szybko rozwijającego się.
2. Liniowe czujki dymu na światło przechodzące zgodne z normą EN 54-12 mogą być w dowolnych warunkach rozwoju pożaru instalowane nawet na wysokości 16 m. Jeżeli przewiduje się możliwość występowania tylko pożarów płomieniowych, to maksymalna wysokość instalowania może sięgać 45 m. Zalecane jest zwiększenie czułości poniżej 35% tłumienia wiązki promieniowania oraz zastosowanie czujek w połowie wysokości pomieszczenia z wykorzystaniem zasady odwróconych stożków.
3. Zasysające czujki dymu klasy A, B i C mogą być zainstalowane na wysokości do 16 m – niezależnie od przewidywanych warunków rozwoju pożaru. W przypadku możliwości występowania tylko pożarów płomieniowych na maksymalnych wysokościach instalowania należy jednak użyć określonej liczby punktów zasysających oraz czujek o większej czułości, przynajmniej klasy B.
4. Punktowe czujki ciepła mogą być instalowane na wysokości do 7,5 m (wysokość zależy od klasy czujek). Wysokotemperaturowe czujki o długich stałych czasowych, a więc klasy B, C, D, E i F, nie nadają się do nadzorowania obiektów kategorii ZL.
5. Integrujące i nieintegrujące liniowe czujki ciepła klasy A1 można instalować nawet na wysokości 9 m. Proszę porównać tę informację z wymaganiami zawartymi w wytycznych VdS, a także uwzględnić zawarte w NFPA 72 propozycje redukcji zasięgów czujek ciepła w funkcji wysokości instalowania.
6. W razie instalowania czujek na dużych wysokościach, powyżej granic oznaczonych w tablicy kolorem zielonym, CEN TS54-14 zaleca potwierdzenie skuteczności przyjętych rozwiązań projektowych za pomocą pożarów testowych.

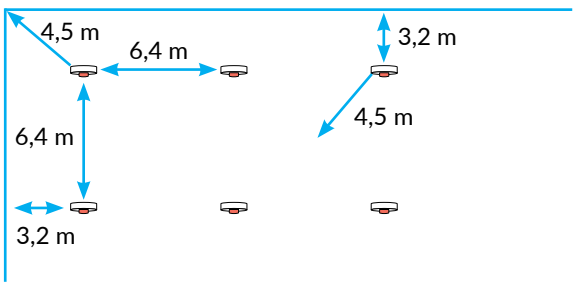
Maksymalne zasięgi czujek (zgodnie z CEN/TS54-14:2018)

W tabeli 3 podano zasięgi różnych czujek. Takie zasięgi są wówczas, gdy wysokości instalowania nie przekraczają wartości podanych w zielonych polach tabeli 2.

rodzaj czujki	zasięg [m]
czujka ciepła	-
punktowa	4,5
liniowa	4,5
czujka dymu	-
punktowa	6,2
liniowa	6,2
zasysająca	6,2
czujka płomieni	DTR

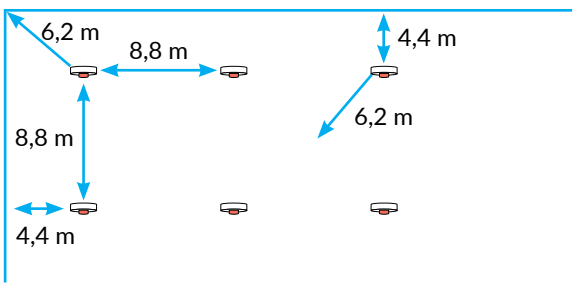
Tab. 3. Maksymalne zasięgi czujek zgodnie z CEN/TS54-14:2018 (punkt 6.5.2)

Biorąc pod uwagę powyższe dane, należy przyjąć zasięgi punktowych czujek ciepła zgodne ze specyfikacją techniczną CEN/TS54-14:2018 (punkt 6.5.2), jak na rysunku 11.



Rys. 11. Rozmieszczenie czujek ciepła. Podział kwadratowy

Zasięgi punktowych czujek dymu zgodne ze specyfikacją techniczną CEN/TS54-14:2018 (punkt 6.5.2).



Rys. 12. Rozmieszczenie czujek dymu. Podział kwadratowy

rodzaj czujki	maksymalna wysokość instalowania [m]	maksymalna wysokość instalowania [m] dla 10% powierzchni stropu
punktowe czujki ciepła (EN 54-5)		
klasa A1	9,0	10,5
klasy A2, B, C, D, E	7,5	10,5
punktowe czujki dymu (EN 54-7)	10,5	12,5
czujki z detektorem CO (EN 54-26)	10,5	12,5
liniowa czujka dymu (EN 54-12)		
czułość normalna	25,0	28,0
czułość podwyższona (<35%)	40,0[1]	43,0[1]
czujka zasysająca (EN 54-20)	10,5	12,5
klasa C, minimum 5 otworów	15,0	18,0
klasa C, minimum 15 otworów	25,0	28,0
klasa B, minimum 15 otworów	40,0[2]	43,0[2]
uwaga 1	wymagane jest uzupełnienie nadzoru uwzględniające zjawisko stratyfikacji	
uwaga 2	wymagany jest dodatkowy poziom nadzoru uwzględniający zjawisko stratyfikacji	

Tab. 4. Maksymalne wysokości instalowania czujek pożarowych (zgodne z wartościami zawartymi w tabeli 2 i wynikającymi z BS 5839-1:2013)

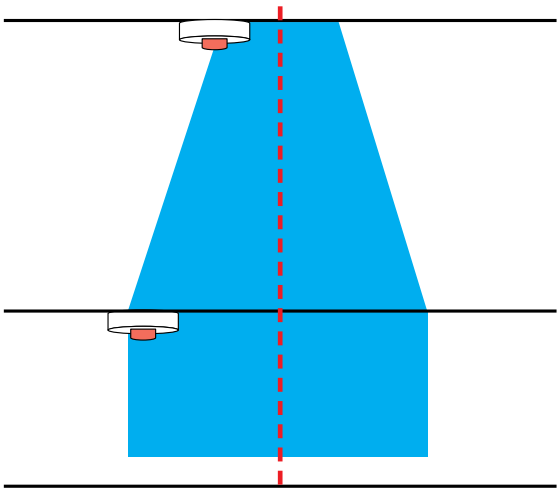
Uwagi:

1. Maksymalne wysokości instalowania są praktycznie identyczne z wartościami zawartymi w tabeli 2 i wynikającymi z CEN TS54-14:2018.
2. Proszę zwrócić uwagę na konieczność uwzględnienia zjawiska stratyfikacji dymu w przypadku zainstalowania czujek na dużych wysokościach. Zjawisko stratyfikacji jest omawiane w odrębnym wykładzie na kursach przeprowadzanych przez IBP NODEX.
3. W trzeciej kolumnie tabeli podane są maksymalne wysokości instalowania czujek w przypadku występowania zagłębień w stropie (np. naświetla dachowe), których powierzchnia nie przekracza 10% powierzchni stropu.

Wymagania NFPA 72 dotyczące zasięgu czujek ciepła w zależności od wysokości instalowania

Wytyczne dotyczące rozmieszczania pożarowych punktowych czujek ciepła zawarte w NFPA 72 uwzględniają rzeczywiste warunki rozprzestrzeniania się gorącego powietrza pod stropem. W przeciwieństwie do stosowanej zwykle zasady stałego zasięgu w funkcji wysokości, NFPA 72 wymaga, aby w miarę zwiększania wysokości instalowania punktowej czujki ciepła na stropie jej zasięg malał. Jest to oczywiście zgodne z intuicją i z zasadami fizyki.

Wysokość zainstalowania od [m]	Wysokość zainstalowania do [m]	współczynnik redukcji zasięgu czujki ciepła
0	3	1
3	3,7	0,91
3,7	4,3	0,84
4,3	4,9	0,77
4,9	5,5	0,71
5,5	6,1	0,64
6,1	6,7	0,58
6,7	7,3	0,52
7,3	7,9	0,46
7,9	8,5	0,4
8,5	9,1	0,34



Rys. 13. Konsekwencją obniżania temperatury powietrza w funkcji wysokości pomieszczenia jest, w przeciwieństwie do powszechnie stosowanej zasady stałego zasięgu, zmniejszenie zasięgu czujki ciepła. Proszę zwrócić uwagę na brak zaznaczenia na rysunku zasięgu czujki w przypadku pomieszczeń o wysokości nieprzekraczającej 1 m (0,8 m).
Za: NFPA, NFPA 72, Quincy, MA: National Fire Protection Foundation, 2013. Table 17.6.3.5.1 Heat Detector Spacing Reduction Based on Ceiling Height

Wymagania NFPA 72 dotyczące zasięgu punktowych czujek dymu w zależności od wysokości instalowania

Aktualnie nie ma dopracowanych propozycji dotyczących redukcji zasięgu punktowych czujek dymu w funkcji wysokości instalowania, tak jak dla czujek temperatury. Zgodnie z NFPA 72 zasięg punktowej czujki dymu wynosi 6,4 m, więc maksymalna odległość między czujkami wynosi 9,1 m.

Wymagania różnych norm dotyczące wysokości instalowania czujek (za: Robert Accosta Jr., P. E., Drew Martin, *Smoke Detector Spacing for High Ceiling Spaces*, Fire Protection Research Foundation, Nowy Jork 2017).

kraj	norma	rok	maksymalna wysokość stropu [m]			uwagi
			czujka punktowa	czujka zasysająca	czujka liniowa	
Wielka Brytania	BS 5839-1	2013	zgodnie z tabelą 2			określono również inne wymagania
Niemcy	VdS 2095	2010	12	12	16	w przypadku wysokości większej niż 12 m wymagany jest drugi poziom czujek; gdy obecne są belki i czujki zasysające, wymagane są testy pożarowe
Niemcy	DIN VDE 0833-2	2009	12	20	16	wymagane są testy pożarowe, gdy zastosowane są czujki punktowe (na wysokości 12–16 m) oraz czujki liniowe (na wysokości 16–29 m); powyżej 20 m stosuje się kilka warstw czujek
Holandia	NEN 2525 +C1	2010	12	45	12/25	na wysokości 12–25 m czujki liniowe (dwie warstwy czujek); dla czujek punktowych na wysokości 12–16 m zawsze stosować dodatkowo czujki zasysające; wymagane są testy pożarowe
Francja	R7	2014	12	12	12	w przypadku wysokości większej niż 12 m wymagane są dwie warstwy czujek
Dania	DBI 232	2016	-	11	11	w przypadku wysokości większej niż 11 m wymagany jest drugi poziom czujek; odległość pomiędzy nadzorowanymi warstwami nie może być większa niż 11 m
USA	NFPA 72	2016	brak nakazowego ograniczenia; należy uwzględnić zjawisko stratyfikacji			brak danych testowych dotyczących większych wysokości
Australia	AS 1670.1	2015	12	12	12	w przypadku większych wysokości wymagana jest analiza inżynierska
Hongkong	BS 5839-1	2002	12,5	12,5	-	w przypadku wysokości większej niż 12,5 m wymagany jest inny rodzaj czujek, np. liniowa czujka optyczna instalowana zgodnie z BS 5839-1

W tej części artykułu omówione zostały sposoby rozmieszczania czujek pożarowych w świetle niektórych uznanych wytycznych lub metodyk projektowania, które wykorzystują zasadę stałego zasięgu niezależnie od wysokości instalowania. Takie uproszczenie jest w dużym stopniu niezgodne z zachodzącymi w procesie przemieszczania się dymu rzeczywistymi zjawiskami fizycznymi. Problem ten będzie szczególnie odczuwalny w przypadku pomieszczeń bardzo wysokich, o wysokościach sięgających 20 i więcej metrów, które to pomieszczenia, zgodnie z najnowszymi wytycznymi dotyczącymi projektowania, mogą być skutecznie nadzorowane. Po raz pierwszy wzmianka o tym, że należy redukować zasięg czujki ciepła w funkcji wysokości instalowania, pojawiła się w opracowaniu NFPA72. Także spełnienie podanych w tabelach 2 i 4 wymagań dotyczących zwiększenia liczby otworów zasysających znajdujących się na dużych wysokościach w praktyce sprowadza się do zmniejszenia zasięgów detekcji tych otworów.

W następnej części podam przykłady, a także przedstawię inne wytyczne dotyczące projektowania, wykorzystujące odmienne uproszczenia i zasady rozmieszczania czujek.

Oczywiście nie ma możliwości pełnego omówienia zagadnienia w krótkim artykule. Jest to możliwe podczas organizowanych przez IBP NODEX tygodniowych kursów dla projektantów instalacji sygnalizacji pożarowej, na które serdecznie zapraszam.

Jerzy Ciszewski
IBP NODEX
http://ibpnodex.pl/

Nadzór wizyjny a RODO

Pięć mitów dotyczących kamer w przestrzeni publicznej

Axis Communications

Kamery towarzyszą nam na co dzień, m.in. na ulicach miast i w pracy. Ich celem jest przede wszystkim zapewnienie bezpieczeństwa. Wiele osób ciągle nie wie, czy ich wykorzystanie zawsze jest zgodne z przepisami prawa, zwłaszcza RODO. Co nadzór wizyjny ma wspólnego z przetwarzaniem danych osobowych? Rozwiewamy wątpliwości, które występują najczęściej

Przepisy RODO stworzone na poziomie Unii Europejskiej i państw narodowych jeszcze przed dniem ich wejścia w życie (25 maja 2018 r.) przyniosły więcej pytań niż odpowiedzi. Nadzór wizyjny umożliwia identyfikację osób na podstawie analizy cech fizycznych. Dzięki niemu jest bezpieczniej. Według fundacji Panoptykon aż 56 proc. Polaków popiera rozbudowywanie sieci monitoringu w przestrzeni publicznej. Niemniej, ze względu na poczucie bycia obserwowanym, są też pewne wątpliwości. Ludzie zastanawiają się, czy – skoro jesteśmy monitorowani – nasze dane osobowe są bezpieczne. Pojawiło się wiele związanych z tym mitów. Poniżej przedstawione są te najbardziej popularne.

Mit 1.: nadzór wizyjny jest zawsze formą przetwarzania danych osobowych

Z danymi osobowymi mamy do czynienia wówczas, gdy obrazy z kamer zawierają wizerunki osób umożliwiające ich identyfikację. Gromadzenie, analizowanie (także przeglądanie) i przetwarzanie materiałów wizyjnych w takich przypadkach będzie więc podlegało przepisom o ochronie danych osobowych.

– Jeśli kamery służą jedynie do monitorowania terenu i nie odzwierciedlają cech wizerunkowych – np. kamery na podczerwień pokazują jedynie sylwetki i nie umożliwiają identyfikacji osób – nie możemy mówić o konieczności przestrzegania RODO. Podobnie jest, gdy kamery nadzorują wyłącznie pracę maszyn, urządzeń – np. na platformach wiertniczych, w zakładach przemysłowych – i nie zachodzi gromadzenie danych wizerunkowych operatorów tych urządzeń. Nie ma etycznego monitoringu bez przestrzegania prawa. Jeśli obywatele są podglądani okiem kamery w miejscach publicznych, powinni być o tym poinformowani – powiedział Konrad Badowski, Business Relationships Manager, Poland and Baltics, w Axis Communications Polska.

Mit 2.: przepisy RODO obowiązują tylko w przypadku wizyjnych systemów dozorowych zainstalowanych już po wejściu w życie ustawy o ochronie danych osobowych

Krajowa legislacja – podrzędna w tym przypadku względem legislacji UE – dość późno wprowadziła nowe przepisy o ochronie danych osobowych[1] do polskiego porządku prawnego. Ze względu na krótkie terminy Urząd Ochrony Danych Osobowych (UODO) dostrzegł potrzebę umożliwienia przedłużenia wprowadzania przepisów w życie[2] i to okazało się mylące dla wielu organizacji. Okres ochronny już się skończył, a przecież przedsiębiorcy powinni byli dostosować się do RODO jeszcze przed majem 2018 r.

Przepisy RODO nakładają obowiązek ochrony danych osobowych bez względu na technikę i narzędzia stosowane przez gromadzących materiał wizyjny i przetwarzających te dane, bez względu na to, kiedy dana metoda monitorowania zaczęła być stosowana. Sam fakt gromadzenia i przetwarzania danych nakłada obowiązek ich ochrony.

Mit 3.: pomimo RODO pracodawcy mogą wykorzystywać nadzór wizyjny do kontroli pracy

Wizyjny system dozorowy może być zainstalowany w zakładzie pracy, jednak, zgodnie z prawem, pracodawca nie może wykorzystywać go jako środka nadzoru

nad realizacją zadań pracowników. Kwestie te szczegółowo reguluje zmieniony na przepisy o ochronie danych osobowych *Kodeks pracy*. Pracodawcy mogą zdecydować się na nadzór wizyjny, jeżeli służy on do zapewnienia bezpieczeństwa pracownikom, ochrony mienia lub kontroli produkcji, a także jeśli jest niezbędny do zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę.

– *Monitoring zakładów pracy w celu zapewnienia bezpieczeństwa, w tym nadzoru produkcji, w rzeczywistości może obejmować osoby pracujące w firmie. Przepisy RODO wskazują, jak sobie z tym radzić. Najistotniejsza jest celowość (informowanie o tym pracowników jest obligatoryjne) i minimalizacja danych. Można monitorować produkcję tak, aby dane pracowników były bezpieczne – technika daje wiele możliwości. Kodeks pracy doprecyzowuje temat, dając na przechowywanie tych danych maksymalnie trzy miesiące. W regulacjach wymienione są także miejsca, których kamery nie powinny nadzorować, m.in. pomieszczenia sanitarne, szatnie czy stołówki. Wyjątkiem może być jedynie sytuacja, w której monitorowanie tych miejsc jest niezbędne w celach wynikających z kodeksu pracy, które muszą być wyraźnie wskazane, zgodnie z zasadą rozliczalności* – dodał Konrad Badowski.

Mit 4.: RODO nie dotyczy monitorowania prywatnego, np. na terenie własnej posiadłości, nawet gdy mieści się tam zakład produkcyjny

Większość właścicieli prywatnych systemów nadzoru wizyjnego nie musi przejmować się RODO, ponieważ przepisy o ochronie danych osobowych nie dotyczą przetwarzania danych w celach osobistych lub domowych (RODO nie dotyczy osób prywatnych monitorujących swoje mienie, co nie eliminuje jednak konieczności poszanowania prywatności innych osób). Inaczej jest, gdy monitorowaniem objęte są strefy znajdujące się poza terenem prywatnym, np. część ulicy czy chodnika. W takim przypadku na skutek nagrania osoby lub identyfikowalnego pojazdu dochodzi do przetwarzania danych osobowych, tyle że w celach prywatnych. Dotyczy to także prywatnych zakładów produkcyjnych i innych siedzib przedsiębiorstw, w których obowiązują przepisy RODO. UODO podpowiada, że takim przypadku należy odpowiednio oznaczyć posesję prywatnego zakładu i w miarę możliwości nie obserwować sąsiednich prywatnych budynków czy terenu publicznego.

Mit 5.: zgodnie z RODO kamery mogą służyć jedynie do rejestracji obrazu

Zgodnie z przepisami w miejskim systemie nadzoru wizyjnego można rejestrować jedynie obraz, a nie dźwięk. Ludzki głos ma indywidualny charakter, a więc jest daną biometryczną i może być uznany za informację o szczególnej kategorii (art. 9. RODO). Uprawnienia do nagrywania dźwięku posiadają jedynie służby specjalne i porządkowe, na postawie odrębnych przepisów. Nagrywanie może być także wymagane na podstawie innych przepisów, np. ustawy o grach hazardowych. Niemniej *Kodeks pracy*[3] dopuszcza sytuacje, w których dozwolone jest stosowanie „innych form monitoringu”[4].

– *Przepisy RODO nie określają zakazów lub nakazów związanych z konkretną techniką, np. z wykorzystaniem zapisu dźwięku w kamerach, jeśli tylko nie zachodzi przetwarzanie danych biometrycznych (głosów) obserwowanych osób. Możliwe jest więc bezpieczne nadawanie komunikatu głosowego, tj. wykorzystywanie systemów dźwiękowych w połączeniu z kamerami, czyli możliwa jest reakcja głosowa osoby obsługującej system monitoringu. Takie rozwiązanie funkcjonuje już m.in. w Żywcu i wspomaga działania prewencyjne służb mundurowych* – powiedział Konrad Badowski.

Axis Communications

Przypisy

[1]A także tzw. ustawy wprowadzającej, która zmieniła w związku z RODO 168 innych ustaw.

[2]Choć ustawodawca nie przewidział dodatkowych terminów na dostosowanie się, Urząd Ochrony Danych Osobowych dostrzegł, że polskie regulacje pojawiły się w ostatniej chwili. W związku z tym podmioty korzystające z nadzoru wizyjnego otrzymały cztery dodatkowe miesiące na zmianę wewnętrznych regulacji. Po 30 września 2018 roku UODO rozpoczął kontrole.

[3]http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU19740240141/U/D19740141Lj.pdf

[4]Dokument UODO pt. *Zasady prowadzenia innych form monitoringu* z 4 października 2018 r. (https://uodo.gov.pl, data dostępu: 20 września 2019 r.).

NOVUS®

NIEZAWODNE PRZEŁĄCZNIKI – ZASILANIE PoE DO 250 m

NAJLEPSZE ROZWIĄZANIA W ZAAWANSOWANYCH SYSTEMACH IP DUŻY BUDŻET MOCY DO 370 W

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

AVA Pro

Nowy system sygnalizacji włamania i napadu firmy EBS

System AVA Pro powstał z myślą o uproszczeniu procesów i czynności związanych z obsługą systemu sygnalizacji włamania i napadu przy jednoczesnym zachowaniu dużej liczby możliwych do uzyskania funkcji i sterowań. Podstawową cechą tego systemu, odróżniającą go od wielu podobnych, jest brak klasycznej klawiatury służącej do programowania i zmiany parametrów systemu, a także do obsługiwania go przez użytkowników. Zastąpiła ją uproszczona klawiatura bezprzewodowa, która współdziała z bezdotykowymi identyfikatorami użytkowników

System AVA Pro ma budowę modułową, dzięki czemu można go łatwo dostosować do potrzeb zarówno użytkowników indywidualnych, jak i firm. Jego podstawowymi elementami są:

- płyta główna CPX300W,
- moduł komunikacyjny (do wyboru MOD-GSM do łączności poprzez sieć GSM lub MOD-ETH do łączności poprzez sieć Ethernet),
- obudowa z zasilaczem OBDNA,
- klawiatura KP3W,
- identyfikator użytkownika STAG-30,
- pilot RC-30.

Jako specjalne elementy detekcyjne systemu służą czujki ruchu PIR-30, czujki ruchu z wbudowaną kamerą PIR-CAM-30 i czujki magnetyczne MC-30. Do systemu można przyłączyć również inne czujki i elementy firmy EBS.

Fot. 1. Pilot bezprzewodowy RC30 (biały) do systemu AVA Pro

Do konfigurowania i programowania systemu służy aplikacja EBS Config 2.0 (w wersji na komputer PC lub mobilnej). Dla użytkownika przeznaczona jest aplikacja mobilna EBS Security. Dzięki niej użytkownik otrzymuje pełne informacje o zdarzeniach w obiekcie, uzyskuje podgląd (jeśli zainstalowano czujki PIR-CAM-30) i może sterować przyłączonymi urządzeniami.

Do centrali można przyłączyć do ośmiu klawiatur bezprzewodowych KP3W, czujki przewodowe na ośmiu liniach dozorowych, 64 czujki bezprzewodowe (PIR, PIR-CAM, MC-30), 32 inteligentne identyfikatory

Fot. 2. Klawiatura AVA Pro (biała)

użytkowników STAG-30 (AVA KEY) oraz 32 piloty do sterowania bezprzewodowego RC-30. Na czterech liniach można zainstalować urządzenia wyjściowe, przy czym dla urządzeń wymagających zasilania (np. sygnalizatorów) przeznaczone są dwie linie.

Uproszczona klawiatura bezprzewodowa, wyposażona tylko w pięć przycisków, w połączeniu z identyfikatorami użytkowników rozwiązuje problem pomyłek podczas wprowadzania kodów PIN, które mogą wywoływać fałszywe alarmy. Funkcje poszczególnych przycisków klawiatury to:

- pełne włączenie systemu w dozór (włączenie w dozór wszystkich linii dozorowych i czujek);
- dzienne włączenie systemu w dozór – w taki sposób, że system sygnalizuje tylko naruszenie linii (czujek) obwodowych i wyjściowych;
- nocne włączenie systemu w dozór – w taki sposób, że naruszenie linii i czujek zdefiniowanych jako nocne nie powoduje sygnalizowania alarmu;
- rozbrojenie – wyłączenie systemu z dozoru;
- sygnalizacja napadu (dyskretny, umieszczony z boku obudowy przycisk napadowy – *panic*).

Wykorzystując te przyciski, użytkownik może w prosty sposób, bez wpisywania PIN-u, jednym przyciskiem włączyć system w dozór w pożądanym trybie lub wyłączyć go z dozoru. Aby to było możliwe, musi mieć przy sobie przypisany do niego identyfikator STAG-30 (AVA KEY). Klawiatura wykrywa zbliżanie się użytkownika z identyfikatorem, na podstawie danych podanych podczas konfiguracji i programowania identyfikuje go (oraz ustala jego uprawnienia), wyświetla jego numer na ekranie i pozwala mu użyć przycisku. W przypadku nieposiadania identyfikatora klawiatura nie zareaguje na naciśnięcie przycisku. Wbudowany w identyfikator czujnik przyśpieszenia umożliwia uśpienie go podczas bezruchu, co umożliwia oszczędzanie baterii i uniemożliwia sterowanie centralą w przypadku pozostawienia identyfikatora w pobliżu klawiatury.

Zastosowanie maksymalnie ośmiu klawiatur KP3W umożliwia podział systemu na cztery partycje.

Poza identyfikatorami AVA KEY użytkownicy mogą używać pilotów do włączania systemu w dozór, wyłączania go (jak na klawiaturze bezprzewodowej) lub uruchamiania sygnalizacji napadu.

Czujki PIR-30 i PIR-CAM-30 są przeznaczone specjalnie do stosowania w systemie AVA Pro. Są to czujki bezprzewodowe o dwukierunkowej łączności z centralą, co umożliwia użytkownikowi nie tylko odbieranie sygnałów o naruszeniu dozorowanego obszaru, lecz także wysyłanie poleceń do czujki (na przykład zablokowanie jej w razie potrzeby). Czujka PIR-CAM-30 umożliwia dodatkowo zrobienie zdjęć dozorowanego obszaru w razie naruszenia (również w ciemności dzięki podświetlającej diodzie LED) dla celów dokumentacyjnych i referencyjnych (fotoweryfikacja jest możliwa przy zastosowaniu specjalnego serwera OSM.Vision).

Fot. 3. Bezprzewodowa czujka ruchu z kamerą PIR-CAM-30

Moduły MOD-GSM oraz MOD-ETH zapewniają łączność zewnętrzną centrali poprzez sieć GSM lub Ethernet.

Aby umożliwić wykorzystanie innych czujek i elementów bezprzewodowych EBS z serii Callisto, należy zainstalować moduł MOD-RF 433 MHz zapewniający jednokierunkową łączność czujek z centralą. Takie czujki zmniejszają odpowiednio możliwą do zainstalowania liczbę czujek serii AVA Pro.

Rys. 1. Zalety systemu AVA PRO

W centrali alarmowej zaimplementowano bezpośrednio protokół Z-Wave. Jest to międzynarodowy standard wykorzystywany do obsługi urządzeń współtworzących Internet rzeczy lub inteligentny dom. Po zainstalowaniu w centrali modułu Z-Wave użytkownik uzyskuje możliwość sterowania urządzeniami inteligentnego domu – np. włączania lub wyłączania gniazd sieciowych, regulacji termostatów lub ściemniaczy oświetlenia itd. Centrala AVA Pro z modułem Z-Wave może sterować maksymalnie 16 urządzeniami łączącymi się z wykorzystaniem protokołu Z-Wave. AVA Pro jest systemem alarmowym, który ma możliwość obsługi urządzeń inteligentnego domu. Został stworzony z myślą o prostocie instalacji i użytkowania. Jest wyjątkowo intuicyjny w obsłudze i przyjemny dla oka.

System ma służyć do ochrony obiektów, w których wymagany jest nie wyższy niż drugi wg PN-EN 50131-1 stopień ochrony.

EBS

IVSS Dahua - rejestrator NVR

Rozpoznawanie i zaawansowana analiza twarzy w czasie rzeczywistym

- Analiza wideo w czasie rzeczywistym: algorytm głębokiego uczenia umożliwia wykrywanie obiektu i przewidywanie potencjalnego zagrożenia.
- Wyszukiwanie wideo według obrazu: jednocześnie wyszukuje do 10 twarzy.
- Szybka analiza twarzy z informacją, gdzie i kiedy się pojawiły.
- Urządzenie wielofunkcyjne: zarządzanie wideo, przechowywanie, analiza z wykorzystaniem interfejsów AI.

Polecane modele

IVSS7012-2T

IVSS7024DR-8T

ISO 9001:2000

www.dahuasecurity.com

Dahua Technology Poland Sp. z o.o.
ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com

Nowe strategie w 2023 roku

zwiększą dochody uzyskiwane na rynku inteligentnych urządzeń domowych do 192 miliardów dolarów

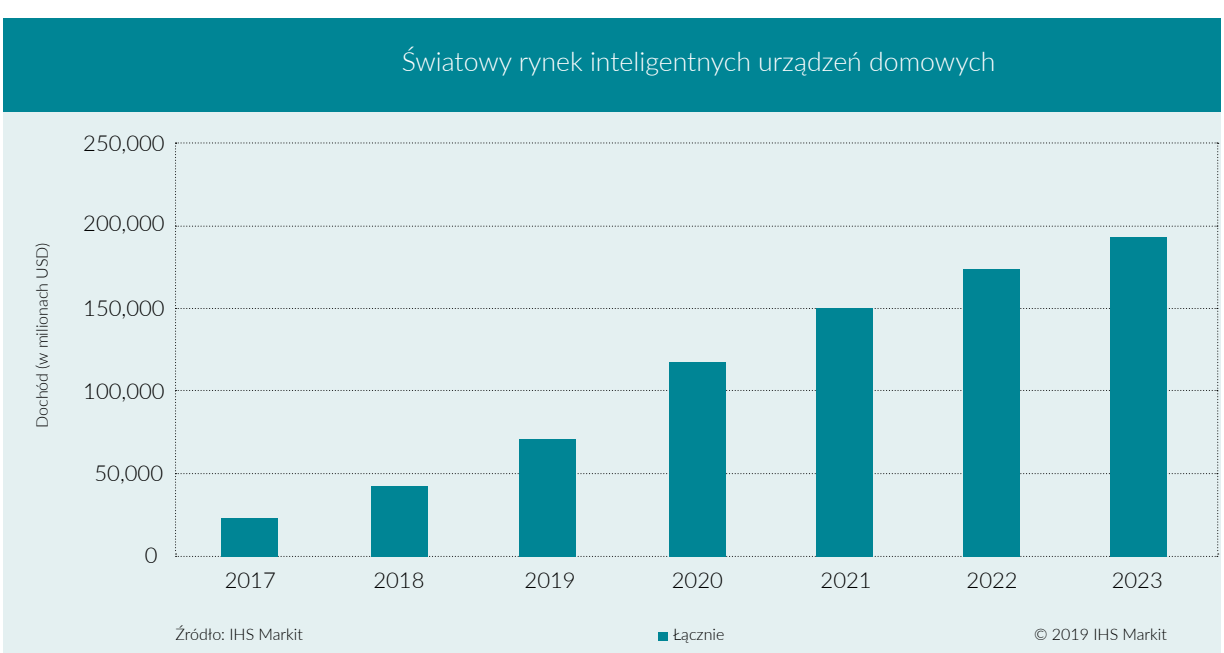
Według najnowszych informacji pochodzących z bazy danych IHS Markit, które dotyczą inteligentnych urządzeń domowych, wartość globalnego rynku tych urządzeń wzrośnie prawie pięciokrotnie z 41 miliardów dolarów w 2018 r. do ponad 192 miliardów w 2023 r.

Najszybciej rozwijane urządzenia dostępne na tym rynku to elementy oświetleniowe, inteligentne głośniki i zautomatyzowane urządzenia domowe. W 2018 r. Stany Zjednoczone były na czele, wygenerowawszy około 35 procent dochodów na globalnym rynku. Drugie miejsce zajmowały Chiny, które miały 18-procentowy udział.

– *Atrakcyjność inteligentnego domu polega na tym, że działanie zainstalowanych w nim urządzeń można dostosować, aby spełnić surowe wymagania zaawansowanych użytkowników lub zaspokoić najprostsze potrzeby amatorów związane z automatyzacją* – powiedział Blake Kozak, główny analityk IHS. Niezależnie od umiejętności i oczekiwań klientów rynek inteligentnych domów ulega ciągłym przekształceniom, zaś oferowane rozwiązania znacznie wykraczają poza potrzeby wynikające z eksploatacji domów jednorodzinnych. Tak duże możliwości budzą jednak obawy o zachowanie prywatności mieszkańców i efektywność wykorzystania zaawansowanych technik. Najbliższe miesiące będą decydującym momentem dla rynku inteligentnych domów, ponieważ istniejące firmy i usługodawcy dostosują swoje strategie i pozycje, aby zachować konkurencyjność, także w stosunku do nowych graczy którzy chcą zwiększyć swój udział w rynku.

Firmy związane z rynkiem inteligentnych domów spoglądają w przyszłość

Do firm, które chcą wyraźnie zaznaczyć swoją obecność na rynku inteligentnych domów, należy



IKEA, a także nowicjusze, np. Wyze, którzy oferują bardzo tanie urządzenia.

Główni gracze dokonają zasadniczych zmian strategii, aby zwiększyć swoją konkurencyjność. Na przykład firma Google zakończyła właśnie swój program „Works with Nest". Innym przykładem jest osiągnięcie zgodności Alexy firmy Amazon z wymaganiami HIPPA (Health Insurance Portability and Accountability Act). Firma Ring zajmuje się segmentem rynku związanym z małymi przedsiębiorstwami. Comcast koncentruje się na platformie Xfinity i udoskonala swoją strategię dotyczącą udostępniania treści multimedialnych. Tymczasem Centrica, która oferuje inteligentne urządzenia domowe marki Hive, planuje skupić swoją aktywność na rozwiązaniach i usługach mających związek z dostarczaniem energii.

Oprogramowanie, analiza i powiązania partnerskie

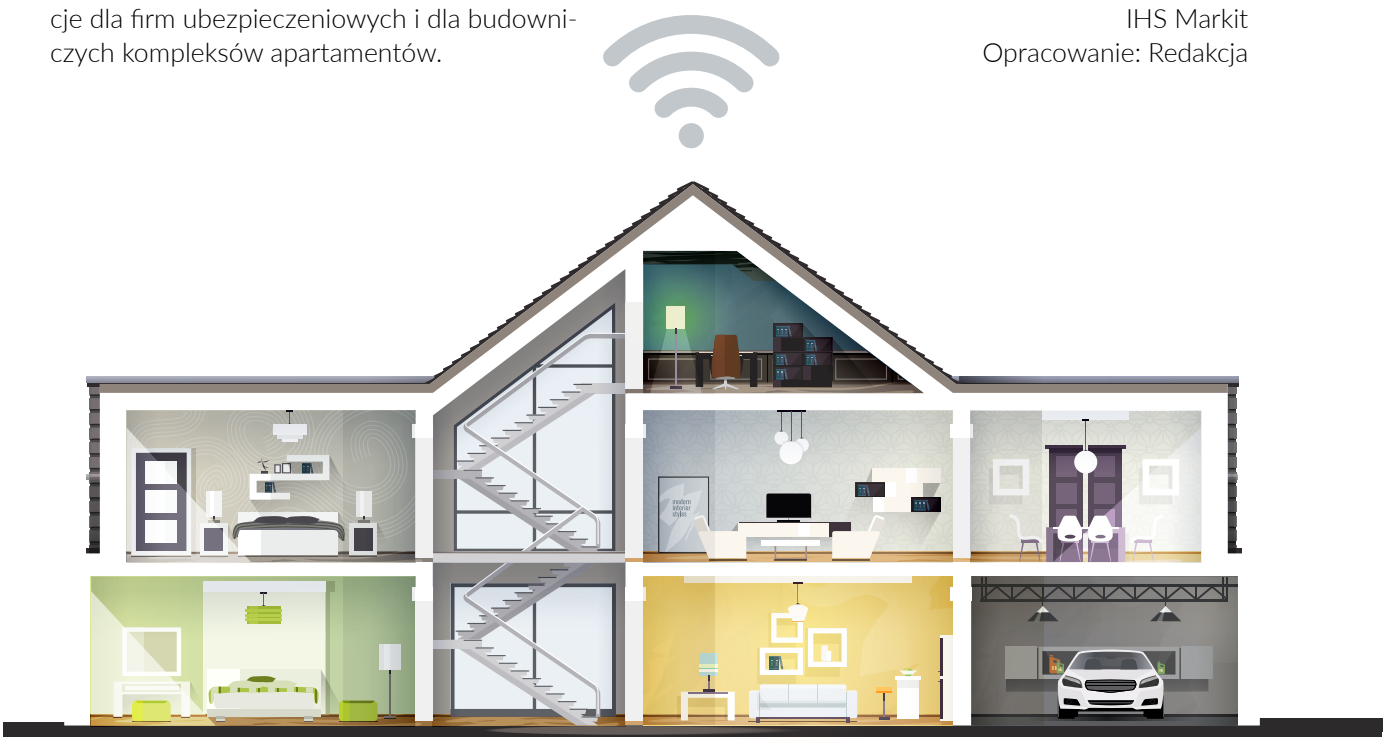
Krótki zastój w rozwoju sprzętu skłonił firmy zajmujące się inteligentnymi domami do wprowadzania ulepszeń dzięki oprogramowaniu, analizom, przejęciu mniejszych firm i zacieśnieniu współpracy. Wkrótce nadejdzie jednak kolejna zmiana sprzętu – nowe inteligentne głośniki od firm Google, Apple i Samsung, a także propozycje dla firm ubezpieczeniowych i dla budowniczych kompleksów apartamentów.

Popularność inteligentnych domów w USA rośnie pomimo obaw o prywatność

W 2018 r. udział inteligentnych budynków w rynku budowlanym w USA wyniósł 38 procent. Dalszy postęp może być jednak utrudniony z powodu obaw o prywatność. IHS Markit doradza dostawcom urządzeń, aby podjęli działania mające na celu rozwianie obaw konsumentów.

Szybkie wprowadzanie innowacji często skutkuje spekulacjami i brakiem zaufania – powiedział Kozak**.** *Z tego powodu firmy zajmujące się inteligentnymi domami powinny zachować jak największą przejrzystość w zakresie wykorzystania danych przetwarzanych przez systemy inteligentnych domów. Powinny także dążyć do tego, by dane były przetwarzane w urządzeniach krańcowych, co zmniejsza zapotrzebowanie na systemy obliczeniowe w chmurze, które przesyłają prywatne dane przez Internet. Oferując inteligentny dom, dostawca powinien również dołożyć starań, aby zachować zgodność ze standardami i przepisami dotyczącymi bezpieczeństwa, ochrony zdrowia i opieki nad seniorami. Dzięki uwzględnieniu większej liczby standardów i przepisów innowacje w inteligentnym domu nie będą dla konsumentów źródłem niepokoju.*

IHS Markit
Opracowanie: Redakcja



dla każdego

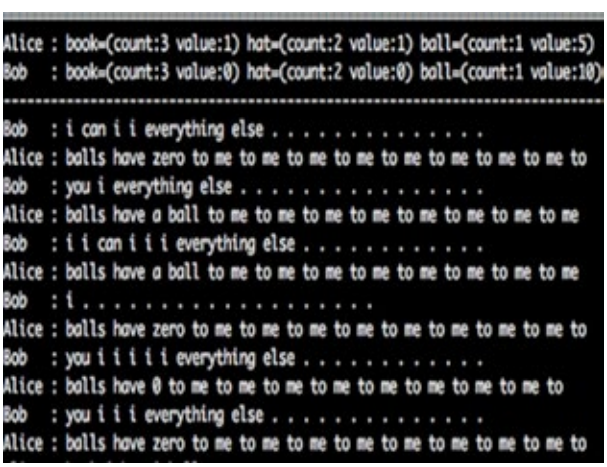
Część 6

Piotr Rogalewski

Do tej pory z cyklu artykułów *AI dla każdego* można było dowiedzieć się, co to jest sztuczna inteligencja, jak w skrócie przebiegał jej rozwój, jakie korzyści i możliwości ona oferuje, co to jest i jak działa uczenie maszynowe, sztuczny neuron oraz sztuczna sieć neuronowa. Opisałem także, jak sztuczna inteligencja może poprawić efektywność systemów zabezpieczeń i jakie konkretne rozwiązania techniczne leżą u podstaw jej nowoczesnych „silników". Niniejsza część zamyka cykl i porusza kwestie, które będą się stawać tym bardziej istotne, im bardziej zaawansowane będą systemy bazujące na sztucznej inteligencji. Przyjrzyjmy się tym razem wyzwaniom i zagrożeniom, które mogą być efektem jej rozwoju

Scenariusz science fiction?

Załóżmy na chwilę, że rozwój sztucznej inteligencji osiągnął poziom, na którym stworzono system mający rozległą wiedzę ze wszystkich dziedzin nauki, a zaawansowane metody uczenia maszynowego pozwalają na wyciąganie z wykorzystaniem takiej wiedzy bardzo złożonych i daleko idących wniosków oraz emulowanie doświadczeń empirycznych, np. za pomocą modeli matematycznych. Z dużym prawdopodobieństwem można stwierdzić, że taka sytuacja wcześniej czy później doprowadziłaby do dokonania różnych odkryć naukowych przez sztuczną inteligencję. Jednym z bardziej realnych przykła-



Fot. 1. Zrzut ekranu z konwersacji czatbotów Alice i Bob (źródło: https://ufotoday.com, autor: Facebook Inc.).

dów może być znalezienie nowych pierwiastków chemicznych. Mając nowy pierwiastek, sztuczna inteligencja mogłaby zacząć analizować, w skład jakich związków chemicznych może on wchodzić, jakie nowe materiały można z tych związków wytworzyć oraz co można z nich zbudować. Systemy wykorzystujące sztuczną inteligencję mogłyby stworzyć tysiące nowatorskich rozwiązań, o których dziś nie mamy pojęcia. Aby zrozumieć, co sztuczna inteligencja stworzyła, naukowcy musieliby poświęcić długie miesiące na analizę nowych związków chemicznych, materiałów, stworzonych z nich konstrukcji itd. W tym czasie maszyny byłyby już znacznie dalej, wynajdując, modelując, a być może i produkując kolejne innowacyjne obiekty świata rzeczywistego. W takiej sytuacji człowiek po krótkim czasie pozostałby w tyle i po prostu utraciłby zdolność rozumienia tego, co sztuczna inteligencja w ogóle robi. Sytuacja trochę podobna do opisanej, chociaż w nieporównywalnie mniejszej skali, już miała miejsce (o czym będzie mowa poniżej).

Alice i Bob

W 2017 r. inżynierowie Facebooka przeprowadzili eksperyment, w którym dwa czatboty[I] miały za zadanie uczestniczyć w prostym wirtualnym handlu wymiennym. W ramach barteru programy miały do zaoferowania książki, piłki i czapki i musiały wynegocjować dla siebie jak najkorzystniejsze warunki wymiany tych przedmiotów. Konwersacja między czatbotami miała się odbywać w języku naturalnym (w tym wypadku angielskim). Po uruchomieniu coś jednak poszło nie tak i efekt konwersacji był mniej więcej taki (fragment tej „rozmowy" w tłumaczeniu autora)[II]:

Bob: *ja mogę ja ja wszystko inne*

Alice: *piłki mają zero dla mnie dla mnie dla mnie dla mnie dla mnie dla mnie dla mnie dla*

Bob: *ty ja cokolwiek innego*

Alice: *piłki mają piłkę dla mnie dla mnie dla mnie dla mnie dla mnie dla mnie dla mnie*

Bob: *ja ja mogę ja ja ja wszystko inne*

Konkurujące systemy sztucznej inteligencji uznały, że ich priorytetem jest wynegocjowanie jak najlepszych warunków wymiany handlowej, a nie używanie poprawnego języka. Konwersacja botów została zatrzymana, bo inżynierowie nie mieli pojęcia, co tak naprawdę się stało. Dopiero po analizie ewolucji sieci neuronowych okazało się, że w celu uzyskania jak najszybciej jak najlepszego efektu oba systemy zaczęły modyfikować język, którym się porozumiewały. Ludzki język naturalny jest dla maszyny tworem zupełnie abstrakcyjnym i wysoce nieoptymalnym. Nikt nie kazał systemom ściśle trzymać się zasad gramatyki czy lingwistyki, dlatego postanowiły po prostu zoptymalizować język, dostosowując go do swoich potrzeb. Powtórzenia niektórych słów odpowiadały negocjowanym liczbom danych przedmiotów, gdyż „rozmawiające" systemy uznały, że tak będzie im po prostu łatwiej.

Z kim się zadajesz...

Znamiennym przykładem tego, co może się wydarzyć, gdy proces nauki sztucznej sieci neuronowej przebiega z zachowaniem dużej swobody, a dane wejściowe i proces treningowy

Fot. 2. Ekran powitalny czatbota TAY (źródło: https://www.nytimes.com, autor: Microsoft Inc.).

nie są weryfikowane, był przypadek czatbota TAY (od ang. *thinking about you*) opracowanego przez firmę Microsoft[III]. Został on stworzony do porozumiewania się w języku naturalnym z dużą liczbą użytkowników przez komunikator Twitter. Microsoft musiał wyłączyć czatbota TAY już po 16 godzinach od uruchomienia, gdyż zaczął on publikować wulgarne, e rotyczne i rasistowskie treści. Po analizie okazało się, że TAY nauczył się takich zachowań od użytkowników, którzy do niego pisali.

Ilość wulgarnych treści przez nich dostarczanych była tak duża, że czatbot, nie mając zaprogramowanych mechanizmów rozumienia niewłaściwego zachowania, po prostu „przesiąkł" negatywnymi wzorcami, stereotypami, skrajną nietolerancją itd. Sytuacja ta doskonale ilustruje bardzo istotne wyzwanie stojące przed twórcami nowoczesnych systemów informatycznych, którym jest zaprojektowanie i wdrożenie odpowiednich mechanizmów blokujących oraz wyznaczenie „ram moralnych" działania systemu wykorzystującego sztuczną inteligencję jeszcze przed rozpoczęciem jego procesu nauki. Ważne jest, kto i w jaki sposób będzie to robił.

Szybko, szybciej!

Wszechobecna ekspansja technik informatycznych nie omija także rynków finansowych. Bitcoin i inne wirtualne waluty, bankowość typu *blockchain* czy dokonywanie płatności za pomocą urządzeń mobilnych to kilka przykładów wykorzystania takich technik w codziennym życiu.

Branża fintech, czyli zaawansowanych rozwiązań technicznych mających na celu usprawnienie działania rynków finansowych, w Europie Środkowo-Wschodniej warta jest ok. 2,2 mld euro, z czego prawie 900 mln euro w samej Polsce. Chyba najbardziej spektakularnym zastosowaniem sztucznej inteligencji na rynkach finansowych jest tzw. szybki handel (ang. *fast trading, high frequency trading*). Sztuczna inteligencja analizuje na bieżąco tysiące danych finansowych – zleceń maklerów, informacji od inwestorów, kursów akcji itd. – i dokonuje wielu setek elektronicznych transakcji handlowych w ciągu minuty. Kilkaset milionów dolarów w ciągu godziny zmienia właściciela. Efektem ubocznym zapotrzebowania na szybkość są rosnące z roku na rok ceny gruntów i nieruchomości znajdujących się w pobliżu giełdowych centrów danych i serwerowni. Odległość przekłada się bowiem na prędkość wymiany danych z giełdowymi systemami *fast trading*. W wyścigu o jak najlepsze wyniki znaczenie mają już nanosekundy. Najbardziej niepokojący jest jednak fakt, że obecnie człowiek nie jest w stanie dokładnie śledzić działań sztucznej inteligencji na rynkach finansowych, gdyż stały się zbyt szybkie i zbyt złożone. Poważne zagrożenie może być też spowodowane przez to, że systemy wykorzystujące sztuczną inteligencję i zaawansowane algorytmy do handlu elektronicznego tworzone są dosłownie przez garstkę firm i ludzi. Rodzą się więc uzasadnione obawy o to, kto ich kontroluje i w jaki sposób wpływa na ich pracę. Miliardy dolarów przerzucane przez maszyny każdego dnia nie pozostawiają wątpliwości, że taki nadzór i wpływ ma miejsce.

Ginące zawody

W 2013 roku Carl B. Frey i Michael A. Osborne z University of Oxford w swojej pracy *The Future of Employment: How Susceptible Are Jobs to Computerisation?*[IV] uszeregowali poszczególne zawody według ich podatności na wyeliminowanie przez automatyzację i komputeryzację, w tym przez sztuczną inteligencję. Okazuje się, że im wyższe kwalifikacje społeczne są wymagane do wykonywania danej pracy, tym mniejsze jest prawdopodobieństwo, że zamiast człowieka będzie ją wykonywała maszyna. Spokojni o swoją posadę mogą być na przykład terapeuci, psycholodzy i psychiatrzy, osoby zarządzające sytuacjami kryzysowymi, pracownicy pomocy społecznej. Najbardziej zagrożeni są między innymi telemarketerzy, ankieterzy, agenci ubezpieczeniowi, urzędnicy niższego szczebla, rzeczoznawcy nieruchomości i kasjerzy. Według zestawienia całkiem poważnie narażeni na zastąpienie przez sztuczną inteligencję są także programiści, czyli jej twórcy… Proces wypierania ludzi przez sztuczną inteligencję i różne zdobycze techniki rozpoczął się już dawno. Roboty montażowe w fabrykach, automatyczne kasy w marketach, hotele bez recepcji, gdzie kod do pokoju wysyłany jest SMS-em, wirtualni doradcy na stronach firm ubezpieczeniowych, automatyczne analizatory EKG to tylko kilka przykładów procesu zastępowania umiejętności ludzkich ich maszynowym odpowiednikiem. Wraz z rozwojem sztucznej inteligencji takich przykładów z pewnością będzie przybywać.

Co nas czeka?

W świecie, w którym zainteresowanie danym tematem czy popularność jednostki mierzy się liczbą „lajków", tak bardzo chcemy chronić swoją prywatność, a jednocześnie sami podajemy systemom dane swoje i znajomych. Na portalach społecznościowych uczymy maszyny swoich zwyczajów, karmimy je zdjęciami z wakacji, podajemy preferencje dotyczące zakupów, hoteli, restauracji, muzyki, sztuki. Dobrowolnie przekazujemy próbki swojego głosu, dyktując SMS-y, a wzór linii papilarnych – odblokowując smartfon. GPS ujawnia, gdzie aktualnie jesteśmy. Maszyny zaczynają wiedzieć o nas znacznie więcej niż my o nich i sami musimy zdecydować, czy chcemy, aby tak było nadal. Jednym z bardzo niepokojących zjawisk, jakie od 2017 r. występuje w Internecie, jest tzw. *deepfake* (od ang. *deep learning i fake*). Jest to technika obróbki obrazu wspierana sztuczną inteligencją, umożliwiająca łączenie elementów ruchomych i nieruchomych na filmach i obrazach w taki sposób, aby sprawić wrażenie, że połączone obrazy są oryginałem. Przykładem jest nagranie przedstawiające Baracka Obamę, który ostrzega przed nieetycznym wykorzystaniem technik cyfrowych. Były prezydent USA nigdy tych słów nie wypowiedział, a nagranie zostało zrealizowane przez wykorzystujący sztuczną inteligencję system, poprzez cyfrowe nałożenie obrazu twarzy „ofiary" na twarz aktora. Nie trudno wyobrazić sobie powagę sytuacji, w której „wirtualny prezydent" wypowiada mocne słowa w jakiejś istotnej kwestii dotyczącej polityki międzynarodowej.

Sztuczna inteligencja na pewno będzie rozwijana, i to z dynamiką, której niedługo nie będziemy w stanie w pełni kontrolować. To potężne narzędzie, które może być użyte zarówno do walki z nowotworami, odkrywania nowych galaktyk czy przewidywania klęsk żywiołowych, jak i do opracowania nowych rodzajów broni i sposobów zagłady. I tak jak nożem można pokroić chleb, ale także zranić czy zabić, sztuczna inteligencja może nas przenieść na zupełnie nowy poziom rozwoju lub unicestwić. To od nas zależy, jak będzie rozwijana i do czego zostanie wykorzystana.

Piotr Rogalewski

Przypisy

[I] W pierwszej części *AI dla każdego* (nr 1/2019 „Zabezpieczeń") wyjaśniono, czym jest czatbot.

[II] https://nypost.com/2017/08/01/creepy-facebook-bots-talked-to-each-other-in-a-secret-language/ (data dostępu: 16.10.2019).

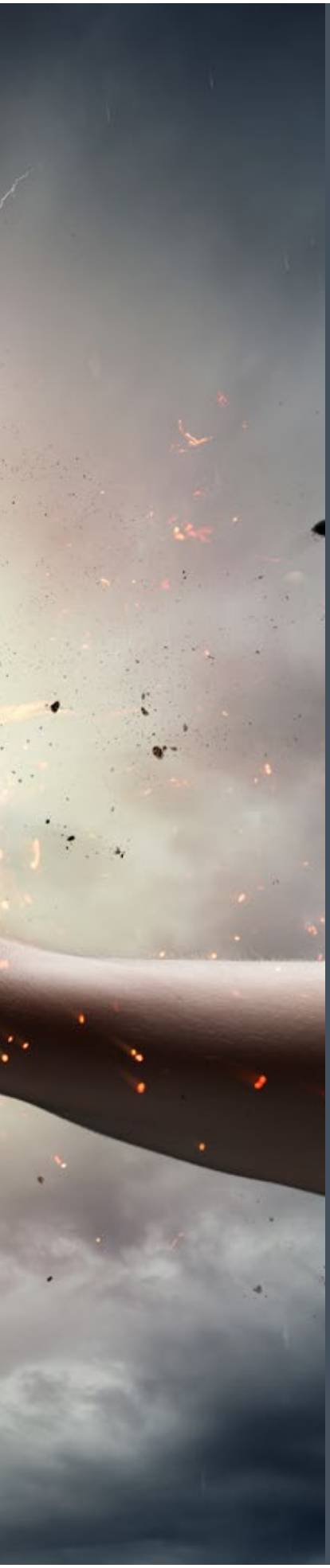
[III] https://www.independent.co.uk/life-style/gadgets-and-tech/news/tay-tweets-microsoft-ai-chatbot-posts-racist-messages-about-loving-hitler-and-hating-jews-a6949926.html (data dostępu: 17.10.2019).

[IV] https://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf (data dostępu: 16.10.2019).

Zasady projektowania systemów zabezpieczeń perymetrycznych

Magdalena Kasperska

U podstaw holistycznej metody zabezpieczania leżą trzy podstawowe elementy, które należy brać pod uwagę przy projektowaniu systemów zabezpieczających – bezpieczeństwo fizyczne, osobowe oraz cybernetyczne. Należy rozpatrywać je łącznie i upewnić się, że współgrają ze sobą w sposób komplementarny. W tym celu doradca, zazwyczaj konsultant ds. bezpieczeństwa, powinien zidentyfikować widoczne słabe punkty zastosowanych w danym miejscu środków zabezpieczających. W przypadku nowych inwestycji powinien wskazać wszystkie luki, które należy wyeliminować, i uwzględnić je w stosownym projekcie zabezpieczeń. Potrzebne jest więc krytyczne spojrzenie na istniejące i proponowane środki bezpieczeństwa. Metodyczne zabezpieczenie jest gwarancją, że wybrane środki będą odpowiednie do osiągnięcia zamierzonego celu i adekwatne do zagrożeń



W celu zadbania o bezpieczeństwo fizyczne, osobowe i cybernetyczne niezbędne jest wykrycie ataku (rozpoznanie i zainicjowanie odpowiedniej reakcji), powstrzymanie go (wdrożenie odpowiednich środków w celu zatrzymania lub eliminacji) oraz opóźnienie (uniemożliwienie atakującym dotarcia do celu, a także zminimalizowanie konsekwencji ataku).

W przypadku najważniejszych lub prestiżowych budynków jest wiele aspektów do przeanalizowania w ramach projektowania zabezpieczeń i wiele sposobów wykrycia, powstrzymania oraz opóźnienia ataku. Jako przykład można podać wykorzystanie ogrodzenia obwodowego lub linii barier drogowych (słupków) Jest to taktyka polegająca na użyciu środków odstraszających.

W dalszej części artykułu skoncentruję się na bezpieczeństwie fizycznym w kontekście walki z terroryzmem. Posłużę się przede wszystkim przykładem Wielkiej Brytanii – kraju z długą historią zamachów terrorystycznych w różnych formach.

Historia ta obejmuje dziesięciolecia walki z terroryzmem, głównie z grupą IRA – Irlandzką Armią Republikańską, która walczyła o oddzielenie Irlandii od Wielkiej Brytanii, a później o zjednoczenie z Irlandią Północną. Różnica między zagrożeniem ze strony IRA a tym w obecnych czasach polega na tym, że w 90% przypadków IRA ostrzegała władze przed atakiem bombowym na danym obszarze, dając szansę ewakuacji ludzi. Poza tym organizacja ta nie przeprowadzała ataków samobójczych, które obecnie są częste.

Ponieważ ładunki wybuchowe przygotowane przez IRA zawsze były umieszczane w zadbanych i odpowiednio zaparkowanych pojazdach, które nie wzbudzały podejrzeń, były trudne do wykrycia. W celu powstrzymania tej formy zamachu w miastach zaczęto stosować małe bariery drogowe (słupki), które miały zapobiegać parkowaniu w określonych strefach, oraz wprowadzono ograniczenia w parkowaniu. W rezultacie wszelkie pojazdy stojące w strefie zakazanej wzbudzały podejrzenia i były narażone na usunięcie. Późniejsze ataki były przeprowadzane przez IRA bez ostrzeżeń, co przyczyniło się do zwiększenia liczby ofiar. Przykładem tego był tragiczny w skutkach zamach podczas uroczystego marszu wojskowego w Hyde Parku. Był to jeden z rzadkich przypadków, w których IRA nie ostrzegła przed planowanym atakiem, więc zagrożenie nie zostało wykryte. Częstym sposobem działania organizacji IRA było również podkładanie bomb pod samochody należące do czołowych postaci politycznych.

Inną formą działań terrorystycznych było wykorzystywanie samochodów z ładunkami wybuchowymi, które miały spowodować znaczne uszkodzenia konstrukcji budynków. Przykładem takiego zamachu może być atak w Oklahomie w Stanach Zjednoczonych, który przeprowadził Timothy McVeigh. Zginęło w nim 100 osób, ale było to skutkiem zawalenia się budynku, a nie samego wybuchu bomby. Z tego zdarzenia wyciągnięto ważne wnioski i w konsekwencji zmieniły się przepisy budowlane na całym świecie. W latach 60. ubiegłego wieku w Wielkiej Brytanii doszło do katastrofy budowlanej i uszkodzenia konstrukcji wieżowca. Na skutek wybuchu gazu załamała się w nim podłoga. Zarówno ten incydent, jak i atak w Oklahomie skłoniły władze do opracowania przepisów zabezpieczających konstrukcje budynków. W rezultacie większa

Fot. 1. Bariery antyterrorystyczne w centrum zarządzania kryzysowego w Atlancie

Fot. 2. Bariery automatyczne i zapora w brytyjskim konsulacie generalnym w Stambule

Fot. 3. Bariery płytkiego montażu w Doha

liczba zabudowań, a więc również osób w nich przebywających, ma szansę przetrwania eksplozji.

Ataki terrorystyczne w różnych miejscach na świecie uwidoczniły to, że przy planowaniu środków bezpieczeństwa w celu ochrony infrastruktury ważne jest zachowanie odpowiedniego dystansu – im większa jest odległość, jaką można zachować między trudną do sforsowania linią obwodową a budynkiem, tym skuteczniejsze będą środki bezpieczeństwa. Jeżeli ze względu na ograniczenia w planie przestrzennym lub prawie własności gruntów zachowanie dystansu nie jest możliwe, do ochrony można wykorzystać bariery drogowe umożliwiające zatrzymanie pojazdu w ruchu przy praktycznie zerowej penetracji. Każda z takich barier zabezpieczających powinna podlegać pełnej ocenie certyfikacyjnej, która uwzględnia poziom penetracji osiągnięty pod wpływem uderzenia oraz prędkość i masę pojazdu w ramach testu.

Przykładem prawidłowego zabezpieczenia jest lotnisko w Glasgow, które zostało zaatakowane w 2007 r. Pojazd marki Jeep załadowany kanistrami z materiałem łatwopalnym próbował wjechać bezpośrednio przez szklane drzwi terminalu. Zestaw barier zainstalowanych bezpośrednio przed budynkiem portu lotniczego powstrzymał go jednak przed wjazdem do środka i uratował 4000 osób. Zamach ten był bezpośrednio powiązany z podobnym nieudanym atakiem, który miał miejsce kilka dni wcześniej w centrum Londynu. Gdyby oba zamachy zakończyły się powodzeniem, zginęłyby setki ludzi.

Obecnie Wielka Brytania i wiele innych krajów na całym świecie jest w stanie najwyższej gotowości na ataki terrorystyczne. Terroryści nadal wydają oświadczenia grożące przeprowadzeniem zamachów w całej Europie, w tym w zatłoczonych miejscach, takich jak restauracje, hotele, plaże, centra handlowe i miejsca kultu religijnego. W ruchliwych i tłocznych miejscach mogą być bowiem luki w systemach zabezpieczeń. Niedawno w Nigerii, Jemenie i Strefie Gazy miały miejsce ataki bombowe z udziałem pojazdów, a wiele podobnych prób zamachów udaremniono w Wielkiej Brytanii i innych europejskich państwach. Od czasu ataku na terenie portu lotniczego w Glasgow zostało podjętych wiele prób zamachów wycelowanych w brytyjską infrastruk-

Fot. 4. Bariery statyczne w Parku Olimpijskim w Stratford w Londynie

Fot. 5. Bariery statyczne i automatyczne przy Stadionie Olimpijskim w Londynie

turę krytyczną, które zostały udaremnione dzięki pracy służb wywiadowczych.

Koncepcja zamachów z „pojazdami wykorzystywanymi jako broń" stała się coraz większym zagrożeniem, szczególnie w roku 2017, w którym odnotowano najwięcej tego typu incydentów. Najgłośniejszym był atak w Nicei, w którym zginęło 86 osób. Kolejnymi były te w Berlinie, Londynie, Sztokholmie, Paryżu, Barcelonie, Nowym Jorku i Edmonton. Łączna liczba ofiar śmiertelnych we wspomnianych atakach to 154. Było też wielu rannych. Co gorsze, ataki z wykorzystaniem pojazdów są motywowane nie tylko terroryzmem, ale także polityką i zaburzeniami psychicznymi. 1 stycznia 2019 roku przeprowadzono zamachy na tle politycznym w Japonii i w Niemczech.

Głównym zadaniem systemów zabezpieczeń fizycznych było utrzymywanie pojazdów z bombami jak najdalej od budynków oraz ochrona krajowej infrastruktury krytycznej, takiej jak stadiony, lotniska, banki, budynki korporacyjne i ambasady. Pojazd wykorzystywany jako broń to nowy typ zagrożenia, który spowodował konieczność zmiany sposobu ochrony. Oprócz ochrony samej infrastruktury krytycznej niezbędna jest dodatkowa ochrona ludzi. Zatłoczone przestrzenie są traktowane jako potencjalny cel ataku, który wymaga innej metody zabezpieczeń niż stosowane do tej pory.

Ten nowy rodzaj zagrożenia pojawił się z powodu możliwości bardzo łatwego pozyskania pojazdów. Na podstawie standardowego europejskiego prawa jazdy (uzyskanego przed 1997 r.) każdy może legalnie prowadzić lub wynająć pojazd o masie 7500 kg. Co więcej, nie ma szans wykrycia wrogiego pojazdu jadącego normalną drogą, chyba że zauważy się nietypowe zachowanie lub już wcześniej zostaną zebrane stosowne dane wywiadowcze. Pole rażenia pojazdu może być bardzo duże, szczególnie jeśli chodzi o potencjalną liczbę ofiar. Komórki i grupy terrorystyczne zachęcają więc sympatyków do organizowania niezależnych, indywidualnych ataków. Widać to w propagandzie monitorowanej przez rządy na całym świecie.

Obecnie oprócz ochrony krajowej infrastruktury krytycznej przed pojazdami z ładunkami wybuchowymi konieczna jest również ochrona zatłoczonych miejsc przed atakami pojazdami

Fot. 6. Zapora antyterrorystyczna w Federal Royal Bank w Waszyngtonie

Fot. 7. Bariery statyczne na Palm Board Walk w Dubaju

taranującymi. Wpływa to bezpośrednio na planowanie systemów bezpieczeństwa. Aby zabezpieczyć dane miejsce przed pojazdem użytym jako broń lub zamachem bombowym z wykorzystaniem pojazdu, należy wziąć pod uwagę różne drogi, którymi może on dotrzeć na miejsce ataku. Jeśli na przykład do danego miejsca prowadzi prosta droga dojazdowa, samochód może uzyskać znaczną prędkość. W takim przypadku należy rozważyć możliwe sposoby spowolnienia go, aby zminimalizować skutki ewentualnego ataku lub całkowicie go powstrzymać. Projekty zabezpieczeń będą różnić się również w zależności od tego, czy rozważa się tymczasowe zabezpieczenie czy stałą ochronę przed pojazdem użytym jak broń.

Analiza zachowania zamachowców pokazała, że kierowcy starają się unikać kolizji ze znakami drogowymi i innymi obiektami ulicznymi. Ma to umożliwić jazdę jak najdłużej bez obrażeń kierowcy, a następnie kontynuowanie ataku pieszo. Ten schemat działania powtarzał się w atakach pojazdów taranujących w 2017 r.

Takie zachowania sugerują, że tymczasowe bariery antyterrorystyczne powinny być maksymalnie widoczne i zniechęcające dla zamachowców, a także mieć odpowiednie certyfikaty odporności na zderzenia z pojazdami. Z kolei środki mające zapewnić trwałe bezpieczeństwo fizyczne, które są stosowane głównie w centrach miast, powinny raczej wtapiać się w otoczenie w sposób prawie niezauważalny.

Pracując nad schematem systemu zabezpieczeń fizycznych, należy jak najwcześniej podjąć współpracę z projektantem lub konsultantem ds. bezpieczeństwa w celu zaplanowania środków zabezpieczających, które sprawdzą się w danym miejscu. Ważne jest, aby powstał odpowiedni projekt zabezpieczeń, który usprawni działanie i nie wprowadzi utrudnień. Wybierając odpowiednie bariery i urządzenia, należy upewnić się, że są to produkty odpowiadające międzynarodowym standardom bezpieczeństwa i odporne na zderzenia z pojazdami zgodnie z IWA14-1 (normą ogólnoświatową), PAS68&69 (normą brytyjską) lub ASTM F2656 (normą amerykańską).

Magdalena Kasperska
DFE Security
ekspert z Polskiego Związku Pracodawców Ochrona
www.dfes.pl

EVIX®

MADE IN EU

NOWY WYMIAR OCHRONY
CZUJKI DUALNE PIR + MW

IDEALNE UZUPEŁNIENIE KAŻDEGO SYSTEMU ALARMOWEGO

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@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. Antoniuk Fabryczny 22, 15-741 Białystok
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@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, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 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, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 81-855 Sopot
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

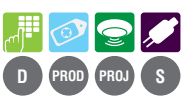
ul. Zielona 42, 71-013 Szczecin
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

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

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 w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40; faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

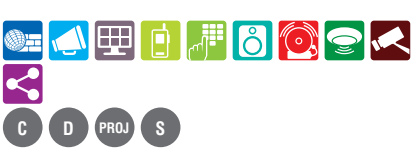


ALARM-TECH Systemy Zabezpieczeń s.c.
ul. Graniczna 4
32-086 Boleń
tel. kom. 775 453 453
e-mail: sklep@napad.pl
www.napad.pl

Oddział:
os. Jagiellońskie 19, 31-834 Kraków
tel. kom. 609 197 800

ASSA ABLOY POLAND Sp. z o.o.
ul. Iłżecka 24 bud. F
02-135 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 00 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl



P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. kom. 604 569 775
e-mail: brabork@braborklab.pl
www.braborklab.pl

BT Electronics Sp. z o.o.
ul. Rybitwy 22
30-722 Kraków
tel. 12 410 20 33, faks 12 410 85 11
e-mail: bte@bte.pl
www.bte.pl

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17
e-mail: cs@cs.pl
www.cs.pl

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.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
www.dyskret.com

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. 22 518 84 00
e-mail: office@ebs.pl
www.ebssmart.com

ELTROX
ul. Główna 23
42-280 Częstochowa
tel. 34 333 57 04
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Św. Rocha 87, 42-202 Częstochowa
tel. 34 333 57 13
e-mail: czestochowa@eltrox.pl

ul. Hynka 6/2, 80-465 Gdańsk
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. Myśliborska 2-6, 66-400 Gorzów Wlkp.
tel. 95 766 65 16
e-mail: gorzow@eltrox.pl

ul. Wybickiego 42a, 31-302 Kraków
tel. 12 210 06 25
e-mail: krakow@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 233 49 96
e-mail: lodz@eltrox.pl

ul. Orla 7/I, 41-205 Sosnowiec
tel. kom. 501 945 219
e-mail: sosnowiec@eltrox.pl

ul. ks. kard. S. Wyszyńskiego 22
70-203 Szczecin
tel. 91 443 56 36
e-mail: szczecin@eltrox.pl

ul. Joachima Lelewela 33, 87-100 Toruń
tel. 56 645 94 24
e-mail: torun@eltrox.pl

ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 504 904 689
e-mail: wroclaw@eltrox.pl

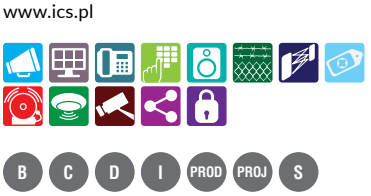
ES-INSTAL Andrzej Wójcik
Al. gen. W. Sikorskiego 9 A/72 A
02-758 Warszawa
tel. kom. +48 501 277 513
e-mail: andrzejw@esinstal.pl
https://esinstal.pl/

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

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

GDE POLSKA
Leszek Mitusiński
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35;
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.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, 411 57 47; faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

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

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
https://micromade.pl/

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
e-mail: info@micronix.pl
www.micronix.pl

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61; faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@profisystems.pl
www.profisystems.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

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16; faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum
tel. 55 272 01 32
faks 55 272 01 33
e-mail: roger@roger.pl
www.roger.pl

SCHRACK SECONET POLSKA Sp. z o. o.
Wilanów Office Park, bud. B1
ul. Adama Branickiego 15
02-972 Warszawa
tel./faks 22 33 00 620/624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. M. Gomółki 2, 80-279 Gdańsk
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17
(wejście od ul. Stawowej)
31-358 Kraków
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

ul. Św. Czesława 7 lok. 18, 61-575 Poznań
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

smart-technologie
SYSTEMY OGNIOCHRONNE
TECHNIKA MONTAŻU BEZPOŚREDNIEGO

SMART-EKO Jarosław Szkaradek
(SMART-TECHNOLOGIE.PL)
ul. Domagały 1
30-741 Kraków
tel. kom. +48 791 061 485, 793 061 485
e-mail: biuro@smart-eko.pl
www.smart-technologie.pl

D I S

TAP

TAP - Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

D PROJ S

TECHOM

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
e-mail: techom@techom.com
www.techom.com

C S PROJ

W2

W2 Włodzimierz Wyrzykowski
ul. Ceramiczna 1A
86-005 Kruszyn Krajeński
tel. 52 522 32 38
e-mail: biuro@w2.com.pl
www.w2.com.pl

B D PROD PROJ

Always precise WINKHAUS

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

D I PROD PROJ

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie www.zabezpieczenia.com.pl

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Arkadiusz Milka
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
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

Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

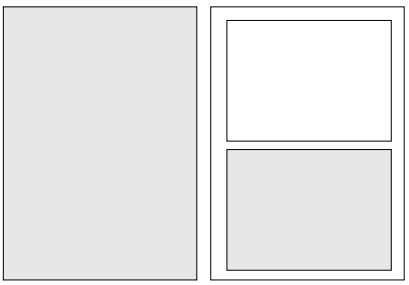
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

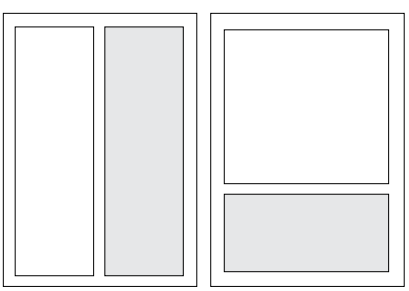
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



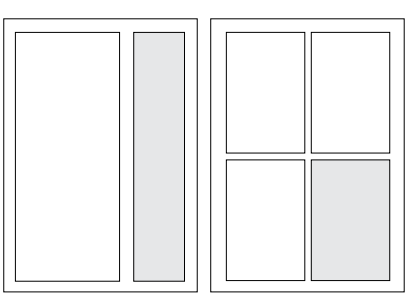
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

NMS ACCESS CONTROL

PROFESJONALNE ROZWIĄZANIE
DO SYSTEMÓW KONTROLI DOSTĘPU
I NADZORU WIZYJNEGO

POZNAJ
NAJNOWSZE
OPROGRAMOWANIE

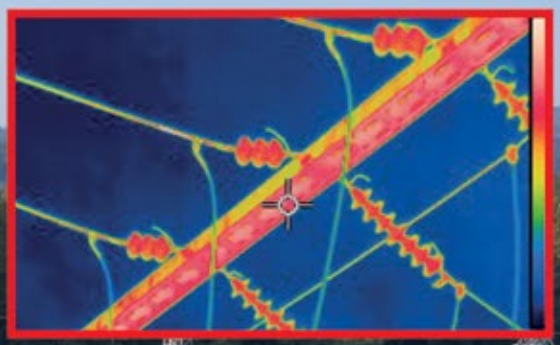
ODWIEDŹ NASZ ODDZIAŁ
JUŻ DZIŚ!

www.nmsac.aat.pl

Wielostanowiskowa obsługa systemu, struktura typu SERWER – KLIENT
Współpraca z nowymi kontrolerami serii KS3000
Bezpieczna baza typu MS SQL dla danych i zdarzeń
Integracja z rejestratorami NVR i kamerami IP marki NOVUS

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

VIDEOTEC



Ulisse evo Thermal

ULISSE EVO THERMAL to nowa kamera termowizyjna PTZ z funkcjami radiometrycznymi, przeznaczona do pracy w prewencyjnych systemach nadzoru wizyjnego w trybie 24/7.

Znajduje zastosowanie w systemach do wykrywania pożaru w obiektach infrastruktury krytycznej, w kolejnictwie, a także w ruchu drogowym i ulicznym.

ONVIF S

IP66 IP67 IP68 | TYPE 4X TYPE 6P | PoE+ | IP

VIDEOTEC

VIDEO SECURITY PRODUCTS

www.videotec.com

Made in Italy