



Zielone Smart City

20 zł
(w tym 8% VAT)



Każde miasto jest inne

Nie od razu Singapur zbudowano. Jakie są perspektywy rozwoju *smart cities* w Polsce?

Wzrost liczby kradzieży

Alert! Inflacja czyni złodzieja. Jak się chronić? Sprawdź metody zapobiegania przestępczości.

Szerokie spojrzenie kamery

Kamery wieloprzetwornikowe rozwiązują wiele problemów związanych z dozorem wizyjnym.

WARSAW SECURITY SUMMIT

Największa
Konferencja
Branży
Zabezpieczeń
Nowa
Formuła

05/06/2023

BEZPŁATNA REJESTRACJA
WARSAWSECURITYSUMMIT.ONLINE



EDITORIAL

Czy miasta muszą być smart?

W historii rozwoju miast widać, że od czasów, gdy ludzkie osady rozrastały się w sposób organiczny i niekontrolowany, powoli zmierzamy w kierunku panowania nad przestrzenią. Dzieje się tak niejako z konieczności. Według danych ONZ już ponad połowa ludności na świecie mieszka w miastach. Do 2050 roku ten odsetek może wynieść nawet 70%. To oznacza kolejne wyzwania: klimatyczne, mieszkaniowe, zdrowotne czy transportowe. Odpowiedzią na te wyzwania jest idea *smart city*.

Naukowcy z Massachusetts Institute of Technology zajmujący się problematyką *smart city* uznali, że inteligentne miasto oznacza połączenie coraz bardziej skutecznych cyfrowych sieci telekomunikacyjnych z różnego rodzaju czujnikami i oprogramowaniem. Inteligencja miasta powstaje zatem jako efekt połączenia wszystkich systemów miejskich: transportu publicznego, dostaw wody i energii elektrycznej, systemu opieki zdrowotnej i socjalnej, zarządzania ruchem miejskim – w jeden sprawnie działający system, którego różne elementy wymieniają się ze sobą informacjami.

Jak z ideą *smart city* radzą sobie polskie miasta? W artykule *Każde miasto jest inne* (str. 20) opowiedzieli o tym przedstawiciele kilku polskich miast intensywnie zaangażowanych w swój technologiczny rozwój. Miasta inwestują w sieci teleinformatyczne, pomiar czystości powietrza, sterowanie transportem, ale nie zapominają też o bezpieczeństwie i zdrowiu mieszkańców. Przykładem jest choćby Wrocław, który wdrożył program teleopieki dla mieszkańców, o czym piszemy w *Głosie branży* (str. 44).

Ostatecznie jednak każde z miast realizuje swoje plany inaczej, ponieważ – jak piszemy w *Raporcie: Zielone smart city* (str. 14) – nie ma uniwersalnego wzoru na inteligentne miasto. Każde z nich ma różne potrzeby i oczekiwania, tak jak różne potrzeby i oczekiwania mają ich mieszkańcy.

Czy jednak wszystkie miasta muszą być *smart*? Tomasz Kulisiewicz, ekspert Ośrodka Studiów nad Cyfrowym Państwem, przyznaje, że nie, jeśli przez *smart city* rozumiemy wyłącznie naszpikowanie przestrzeni publicznej licznymi czujnikami (rozmowa na str. 28). Każde jednak powinno być przyjemne do życia i bezpieczne. Najważniejszy bowiem w całej koncepcji *smart city* jest komfort życia mieszkańców. I w tę właśnie stronę ewoluuje idea – coraz częściej mówi się o *smart city 3.0*, czyli takim mieście, którego władze na pierwszym miejscu stawiają potrzeby obywateli i ich pomysły, a technologia ma być wyłącznie narzędziem do zapewnienia ludziom lepszych warunków życia. I słusznie, jak bowiem stwierdził kiedyś znany amerykański psycholog Rollo May, *technologia to sztuka takiego aranżowania świata, żebyśmy go nie doświadczała*.

Tego sobie i Państwu życzymy...

Redakcja

ZŁOTY PARTNER A&S POLSKA



SREBRNY PARTNER A&S POLSKA



A&S POLSKA WYDANIE ONLINE

www.aspolska.pl/czasopismo

SPIS TREŚCI



Zielone Smart City

8 Produkty Numeru

SMART CITY

- 14 Raport: Zielone smart city
Adela Prochyra
- 20 Każde miasto jest inne
Monika Żuber-Mamakis
- 28 Smart City 4.0
Michalina Nowak
- 34 Smart city: stara idea w nowej odsłonie
Jacek Tyburek
- 38 Inwestycje w monitoring miejski pozwalają zmniejszyć liczbę
niebezpiecznych zautków
Axis Communications
- 40 Hikvision wspiera Smart City 3.0
Michał Swoboda, Hikvision Poland
- 42 SPIN AI – wsparcie dla inteligentnych systemów monitoringu
w miastach
OKE Poland
- 43 Lidar w projektach smart city – najważniejsze korzyści z zastosowania
William Pao, asmag.com
- 44 Głos branży

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-C A RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska
Michalina Nowak

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Bogusław Kalwala

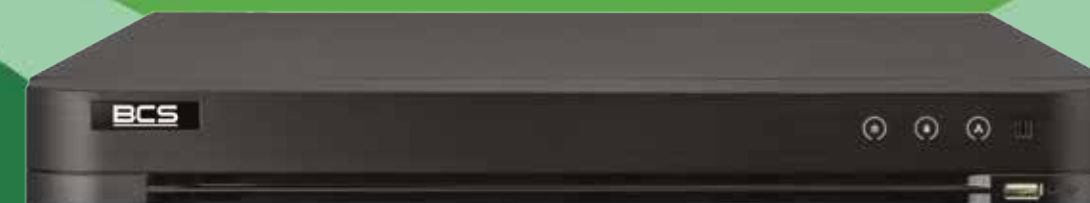
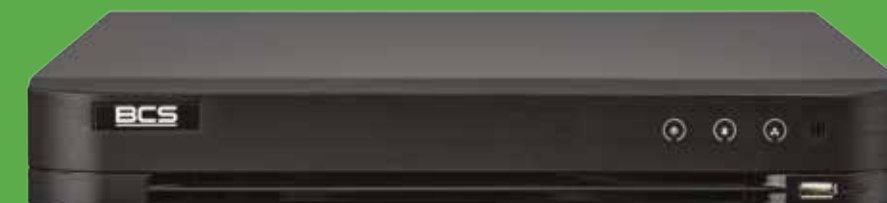
WYDAWCA
SENS Group Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa
www.sensgroup.pl

Redakcja zastrzega sobie prawo
skręcania i redagowania nadesłanych
tekstów. Tytuły i śródtytuły
pochodzą od Redakcji.
Opinie autorów nie muszą być tożsame
z poglądami Redakcji.
Za treść reklam i artykułów partnerów
Redakcja nie odpowiada.
Przedruki tekstów bez zgody Wydawcy
są niedozwolone.

© Copyright by a&s Polska

Rejestratory XVR

Rejestratory XVR serii BCS View z funkcjami AI to nowoczesne podejście do zagadnienia telewizji analogowej wysokiej rozdzielczości. Rejestratory te posiadają funkcje zaawansowanej analizy wideo i oferują funkcjonalności porównywalne z tymi, które dostępne są w rozwiązaniach telewizji dozorowej IP.



» Więcej przeczytasz na stronie 8



www.bcs.pl
www.facebook.com/bcspol



SPIS TREŚCI

RYNEK SECURITY

- 50 Mapa inwestycji
Adela Prochyra
- 52 Branża bezpieczeństwa w Polsce. Raport
Polskiego Związku Pracodawców Ochrona
PZPO
- 54 Lawinowy wzrost liczby kradzieży
Tomasz Grzelak
- 58 Kamery wieloprzetwornikowe
Jan T. Grusznik
- 61 Kamery wieloprzetwornikowe w ofercie
firm BCS i Hikvision
- 62 Integracja systemów zabezpieczeń
Wojciech Pawlica, Dahua Technology
- 63 Bezprzewodowa elektroniczna kontrola dostępu
w budynkach biurowych
Magdalena Madej, Winkhaus Polska Beteiligungs
- 64 Inteligentne budynki numerem 1
na rynku nieruchomości
Secuirtas
- 66 Kontrola dostępu klasy 4 według
PN-EN-60839-1167
Jerzy Taczalski, Ifter
- 68 Jak wybrać system zarządzania szafkami
Nedap Security Management
- 70 Realizacja Varso Tower – najwyższego budynku
w Unii Europejskiej
Schrack Seconet Polska

SYGNALIZACJA POŻAROWA

- 72 Ochrona przeciwpożarowa budynków. Systemy
transmisji alarmów pożarowych
Grzegorz Mroczo
- 76 Kompaktowy system sygnalizacji pożarowej
POLON 3000
Polon Alfa

CYBERBEZPIECZEŃSTWO

- 78 Higiena bezpiecznej pracy zdalnej
Tomasz Dacka

SERWIS INFORMACYJNY

- 82 Nowości produktowe/informacje firmowe
- 88 Centrum Kompetencji: Tajemnica zaginionego
segregatora
Monika Żuber-Mamak



**Polskie profesjonalne
zintegrowane rozwiązania
VMS**
**Ponad 200 000 instalacji
na całym świecie**
**Jesteśmy z Wami od
2003 roku**



www.alnetsystems.com



Najnowsze urządzenia z oferty firm:

Axis Communications, BCS (NSS), EVVA, Hikvision, Nedap Security Management, Schrack Seconet Polska, TP-Link



Axis Communications

Axis Body Worn Live. Streaming z kamer nasobnych w czasie rzeczywistym

Axis Communications przedstawia funkcję AXIS Body Worn Live, która umożliwia strumieniowe przesyłanie wizji, dźwięku i metadanych z kamer nasobnych na żywo. Rozwiązanie wspiera operatorów w podejmowaniu trudnych decyzji w sytuacjach kryzysowych.

AXIS Body Worn Live (BWL) pozwala użytkownikowi kamery na uruchomienie strumieniowego przesyłania danych z jednoczesnymi ich rejestrowaniem. Operator otrzymuje powiadomienie o lokalizacji kamery na podstawie GPS i może w czasie rzeczywistym obserwować sytuację w aplikacji, co umożliwia podejmowanie decyzji na podstawie danych wpływających na bieżąco. Dzięki temu podczas interwencji łatwiej utrzymać bezpieczeństwo pracowników lub przeprowadzić konsultację, która pomoże np. obrać odpowiedni kierunek drogi. Operator może przeanalizować obraz i zwrócić osobie w terenie uwagę na niezauważony obiekt, który warto zabezpieczyć. Transmisja jest szyfrowana na całej trasie, możliwe jest także przypisywanie uprawnień powiązanych z rolami w celu ochrony integralności systemu.

Funkcja działa niezależnie od wybranego systemu zarządzania materiałem wizyjnym lub dowodowym. Strumień danych może być kierowany do jednego lub większej liczby obserwatorów i wyświetlany na komputerach lub urządzeniach mobilnych. Dane są dostępne przez 24 godziny, a buforowanie zapobiega ich utracie w razie przejściowych zakłóceń transmisji. Kamery łączą się przez wstępnie skonfigurowaną sieć Wi-Fi, samo rozwiązanie AXIS BWL działa na platformie Microsoft Azure. AXIS BWL jest w pełni zgodne z wymogami RODO oraz regularnie aktualizowane.



Więcej na:
www.axis.com/pl-pl



BCS

Rejestratory BCS-V-XVR. Analiza wizyjna w rozwiązaniach analogowych

Rodzina rejestratorów XVR serii BCS View z funkcjami AI to innowacyjne podejście do zagadnienia telewizji analogowej wysokiej rozdzielczości. Rejestratory te z zaawansowaną analizą wizyjną oferują funkcjonalności porównywalne z rozwiązaniami rejestratorów sieciowych IP.



Rejestratory obsługują kamery analogowe w rozdzielczości do 8 Mpix oraz oferują możliwość rozbudowy o obsługę dodatkowych kanałów IP (maks. rozdzielczość 8 Mpix). Pracują we wszystkich dostępnych trybach telewizji analogowej HDCVI/AHD/TVI/CVBS, automatycznie określając typ kamery, co znacząco ułatwia instalację.

Podstawową ich zaletą jest obsługa zaawansowanej analizy wizyjnej w kamerach analogowych. Obejmuje ona funkcję ochrony perymetrycznej, w tym przekroczenie linii oraz wtargnięcie w strefę, inteligentną detekcję ruchu reagującą jedynie w przypadku pojawienia się odpowiedniego typu obiektu (człowiek lub samochód). Dostępna jest także funkcja detekcji twarzy.

Z funkcji inteligentnych szczególnie przydatna jest możliwość rozbijania systemu z aplikacji mobilnej BCS View, dostępnej zarówno na systemy iOS, jak i Android. Pozwala to na wyłączenie powiadomień w momencie, gdy wiemy, że alarm nie stanowi powodów do niepokoju. Rejestratory dostępne są w wersjach 4-, 8- i 16-kanałowych.

Więcej na: www.bcs.pl

POLON-ALFA



dobrze zaprojektowane BEZPIECZEŃSTWO

KOMPLEKSOWE SYSTEMY SYGNALIZACJI POŻAROWEJ

- PRODUKCJA • SERWIS • SZKOLENIA
- WSPARCIE TECHNICZNE I PROJEKTOWE

AUTOMATYKA POŻAROWA

POLON-ALFA S.A. | 85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl



EVVA

EMZY EVVA. Automatyczne zamykanie drzwi

Chcesz mieć pewność, że drzwi zewnętrzne i wewnętrzne prowadzące do stref wrażliwych będą blokowane i odblokowywane automatycznie? Umożliwia to wkładka motoryczna EMZY dostarczana przez EVVA Polska.

Zaspokojenie potrzeby bezpieczeństwa w budynkach to także niezawodne rozwiązania, które gwarantują, że drzwi, niezależnie od tego, czy zewnętrzne, czy wewnętrzne prowadzące do stref wymagających kontroli, będą automatycznie zamykane. Elektroniczną wkładkę motoryczną EMZY EVVA wyróżniają m.in. możliwość zdalnego otwierania oraz adaptacja momentu obrotowego. Wkładka motoryczna dopasowuje się do każdej sytuacji, pracując praktycznie z każdym zamkiem drzwiowym, nie wymaga także dużej ingerencji w profil drzwiowy.

Adaptacja momentu obrotowego do 2 Nm oszczędza drzwi i zamek oraz gwarantuje zapas „mocy” potrzebny do otwierania ciężkich i wysokich drzwi. Podczas uruchamiania wkładka poznaje parametry zamka oraz drzwi i dostosowuje do nich swój moment obrotowy.

Dzięki EMZY możliwe jest uzyskanie pełnej informacji o statusie drzwi oraz sterowanie urządzeniem w połączeniu z innymi systemami: przeciwpożarowymi i alarmowymi oraz wyposażeniem technicznym budynku i systemami ewakuacyjnymi.

Więcej na: www.evva.pl



HIKVISION

Kamery IP ANPR (LPR)

Poza katastrofami naturalnymi, błędami ludzkimi i awariami technicznymi infrastruktura krytyczna oraz obiekty wysokiego ryzyka są narażone na inne zagrożenia, w tym kradzież danych lub ataki z użyciem impulsów elektromagnetycznych (EMP).



Kamery sieciowe ANPR firmy Hikvision wyposażone są w technologię rozpoznawania tablic rejestracyjnych pozwalającą na zarządzanie systemem parkingowym i kontrolę przepływu pojazdów.

Najważniejszą funkcją kamer jest rozpoznawanie i identyfikowanie numerów tablic rejestracyjnych zarówno polskich, jak i zagranicznych, a także innych cech pojazdu, m.in. marki, modelu i koloru. Umożliwia to skuteczną

detekcję wjazdu i wyjazdu, monitorowanie zajęcia miejsc parkingowych, a także sterowanie szlabanami i bramami. Ponadto kamery ANPR pozwalają na automatyczną klasyfikację kraju oraz możliwość zdefiniowania białej i czarnej listy do 4000 numerów rejestracyjnych. Urządzenia są przystosowane do pracy autonomicznej bez udziału serwera.

Kamera IP IDS-2CD7A26G0/P-IZHSY typu bullet wykorzystuje algorytmy sztucznej

inteligencji do prawidłowego rozpoznania i klasyfikacji obiektów (człowiek czy pojazd), a także funkcje inteligentnej analizy obrazu (wtargnięcie, przekroczenie linii, wykrycie wejścia/wyjścia).

Kamery IP ANPR znajdują zastosowanie na parkingach, w centrach handlowych, na lotniskach i w budynkach użyteczności publicznej.

Więcej na: www.hikvision.com/pl

LINC POLSKA

iTower® by LINC Polska. Mobilne wieże do monitoringu

Przebudowy, remonty, kontrola prędkości, awarie, braki oświetlenia, imprezy masowe to rzeczywistość każdego miasta. W takich sytuacjach bardzo dobrze sprawdzają się mobilne wieże do monitoringu iTower® by LINC Polska.

Ich założeniem jest:

- **elastyczność wyposażenia** – indywidualnie dopasowane do potrzeb oświetlenie, system monitoringu, kamery do pomiaru prędkości lub temperatury (wykrywanie pożaru);
- **praca w każdych warunkach**, nawet przy braku infrastruktury sieciowej czy energetycznej. Wieże mogą być zasilane energią z 1-3 paneli słonecznych lub z ogniw paliwowych. Przy zasilaniu hybrydowym wieża może pracować autonomicznie nawet przez kilka miesięcy;
- **mobilność** (szybka i łatwa instalacja oraz transport);

- **zdalny dostęp do obrazu z kamer** (wideoweryfikacja), np. w miejskim centrum monitoringu;
- **odstraszenie potencjalnego intruza** przez głośnik zamontowany na szczycie masztu o wysokości 7 m;
- **możliwość uruchomienia usługi** zabezpieczenia obiektu **w ciągu jednego dnia** przez jedną osobę (instalacja wieży zajmuje ok. 15 minut).

Każda wieża jest wyposażona w router zapewniający komunikację bezprzewodową LTE, połączenie Wi-Fi oraz opcjonalny nadzór nad lokalizacją wieży poprzez GPS. Router można wyposażać w dwie karty niezależnych operatorów, tak aby przygotować się na potencjalny

braku zasięgu lub awarii jednego z nich.

iTower® jest idealnym rozwiązaniem do ochrony imprez masowych, koncertów, tymczasowych lokalizacji – budowy dróg, mostów, torów czy rurociągów. iTower® by LINC Polska to mobilność, elastyczność oraz skuteczność w stylu SMART City.

Więcej na: www.linc.pl



iTOWER

TAM GDZIE STANDARDOWE ZABEZPIECZENIA SIĘ
NIE SPRAWDZAJĄ TAM JESTEŚMY MY.

Mobilne rozwiązania do ochrony



WŁASNE ZASILANIE



OSZCZĘDNOŚĆ



MULTISPEKTRALNOŚĆ



WYTRZYMAŁOŚĆ



NIEZALEŻNOŚĆ



BEZPIECZEŃSTWO
DOSTĘPU



NEDAP SECURITY MANAGEMENT

Integracja GANZ CORTROL i Nedap AEOS

W swojej najnowszej wersji oprogramowanie GANZ CORTROL 1.23.0 typu VMS (Video Management System) zostało zintegrowane z systemem kontroli dostępu Nedap AEOS. Ta synergia umożliwia kompleksowe zarządzanie infrastrukturą bezpieczeństwa, zapewniając jednocześnie wygodę i prostotę obsługi.

Od typowych systemów VMS oczekuje się dziś czegoś więcej niż samego wideo. Oprogramowanie GANZ CORTROL w obu wersjach – premier i global – zapewnia natywną, dwukierunkową integrację z systemem kontroli dostępu Nedap AEOS. Lista czytników, które można powiązać z odpowiednimi drzwiami, jest wprowadzana do oprogramowania GANZ CORTROL na etapie konfiguracji.

Natomiast informacje z systemu AEOS można wykorzystać w CORTROL do automatycznego generowania zdarzeń po uprzednim zaprogramowaniu odpowiednich reguł w Konfiguratorze zdarzeń i akcji. Zdarzeniami mogą być różne działania, np. próba nieautoryzowanego otwarcia drzwi wyświetlać będzie obraz z kamery powiązanej z tymi drzwiami, a operator będzie powiadamiany za pomocą komunikatu wyświetlonego na ekranie oraz dźwięku ostrzegawczego.

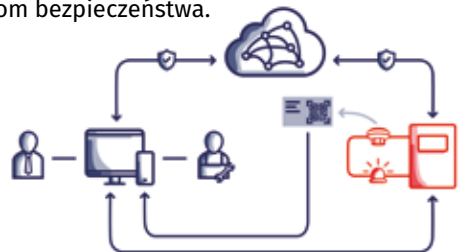
Mapy w CORTROL informują o statusie drzwi i czytników za pomocą tzw. indykatorów zmieniających kolor oraz wygląd w zależności od ich statusu w systemie kontroli dostępu. Powiązanie kamer z określonymi przejściami zapewnia dodatkowe możliwości interakcji na mapie, np. zmiana koloru indykatora kamery alarmująca o wystąpieniu zdarzenia w systemie kontroli dostępu. Więcej na: www.nedapsecurity.com/pl/pl



Schrack Seconet Polska

Platforma serwisowa S2

Certyfikowana (pod względem bezpieczeństwa) platforma chmurowa S2Service umożliwia bezpieczne połączenia z nadzorowanymi obiektami przez VPN. Wszystkie routery pracują w chmurze S2Service i są zarządzane przez producenta, co gwarantuje najwyższy poziom bezpieczeństwa.



Najważniejsze funkcje:

- Najwyższe standardy bezpieczeństwa dzięki szyfrowanym tunnelom VPN i dwuetapowej autoryzacji użytkownika.
- Pełny dostęp do najnowszej dokumentacji produktowej, projektowej oraz informacji serwisowych. Możliwość szybkiego wyszukiwania elementów poprzez kody QR.
- Wbudowane algorytmy do analizy oprogramowania, przyjętych rozwiązań i ich wzajemnej kompatybilności.
- Automatyczna analiza obciążenia systemu. Szczegółowa informacja o możliwościach rozbudowy, elementów wyposażenia zarówno central, jak i peryferyjnych.
- Zdalne zarządzanie zdarzeniami przez Integral Remote zapewnia stały dostęp do wszystkich komunikatów systemowych i stanu systemu w czasie rzeczywistym.
- Automatyczne generowanie protokołów serwisowych, list przetestowanych elementów i list nieprawidłowości.
- Możliwość szybkiego dodania dokumentacji fotograficznej i listy nieprawidłowości do raportu z przeglądu.
- Zarządzanie zadaniami serwisowymi. Łatwe tworzenie zadań na podstawie listy komunikatów zdarzeń z systemu.
- Wsparcie przy instalacji systemu. Montaż i jednoczesna alokacja elementów z wykorzystaniem aplikacji Integral Scan czytującej kody QR elementów. Tak przygotowaną listę elementów można wykorzystać do programowania centrali.

Więcej na: www.schrack-seconet.pl



TP-Link

TP-Link VIGI C240 kopułkowa kamera CCTV, IK10 i IP67

Sieciowa kamera VIGI C240 generuje obraz w rozdzielczości 4 Mpix. Wbudowane diody LED zapewniają kolorowy obraz także w całkowitej ciemności. Urządzenie wyposażono w wodoodporną i pyłoszczelną obudowę spełniającą normy IP67, jest zatem odporne na warunki atmosferyczne. Klasa wytrzymałości mechanicznej IK10 oznacza, że urządzenie jest chronione przed aktami wandalizmu, zapewniając nieprzerwany monitoring w dowolnym miejscu.

Funkcja smart wykrywa osoby oraz pojazdy, ruch, przekroczenie linii, wtargnięcie na obszar, przywłaszczenie lub porzucenie obiektu czy sabotaż kamery. Do skorzystania z funkcji smart nie jest wymagany rejestrator VIGI. Kamera wykorzystuje kompresję H.265+, co zmniejsza obciążenie sieci i obniża koszty monitoringu bez utraty jakości obrazu.

VIGI C240 może być zasilana za pomocą zasilacza 12 V lub dla łatwiejszego montażu również kablem Ethernet (przez PoE). 4-Mpix kamera jest dostępna w dwóch wariantach – z obiektywem o ogniskowej 4 lub 2,8 mm. Dzięki aplikacji VIGI, kamerami z tej serii można w prosty i kompleksowy sposób zarządzać z poziomu smartfona (z Androidem lub systemem iOS). Systemem VIGI można też zarządzać za pomocą oprogramowania przeznaczonego do komputerów oraz rejestratorów NVR.



Wszystkie urządzenia z serii TP-Link VIGI są zgodne ze standardem ONVIF, dzięki czemu współpracują z kamerami i rejestratorami różnych producentów i umożliwiają stworzenie kompleksowego systemu monitoringu. Kamera VIGI C240 została objęta 3-letnią gwarancją producenta.

Więcej na: www.tp-link.com/pl

NOVUS
MANAGEMENT
SYSTEM

INTEGRACJA KONFIGURACJA WIZUALIZACJA SYSTEMÓW BEZPIECZEŃSTWA

NOWA
WERSJA!

NOVUS MANAGEMENT SYSTEM AC
V.5

Integracja z systemem alarmowym SSWiN Satel!

Pełna kontrola nad bezpieczeństwem dzięki integracji z systemami telewizji dozorowej, rozpoznawania tablic rejestracyjnych, kontroli dostępu, rejestracji czasu pracy, sygnalizacji włamania i napadu oraz automatyki budynkowej



JAK TO DZIAŁA?

NMSAC.AAT.PL

NMS AC to profesjonalne polskie oprogramowanie zarządzające systemami bezpieczeństwa w obiektach.

Do nabycia u najlepszych instalatorów!

AAT SYSTEMY BEZPIECZEŃSTWA

PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl



Raport: Zielone Smart City

Nie ma wzoru na *smart city*. W każdym przypadku jest to inna kompilacja pomysłów i rozwiązań z zakresu informacji i technologii. Wybór jest ogromny: inteligentne oświetlenie, zintegrowany system monitoringu wizyjnego, *smart building*, zastosowanie GPS w pojazdach miejskich, nowoczesny system utylizacji odpadów, biletomaty, wypożyczalnie rowerów i hulajnóg, inteligentne karty miejskie, systemy mierzące natężenie ruchu, temperatury czy zanieczyszczenia powietrza, portale zdalnej obsługi mieszkańca i wiele innych. Miasta na całym świecie stosują je wg swoich potrzeb i możliwości, uzyskując różne efekty, skrupulatnie mierzone w rankingach smart. Jak wygląda to w polskich miastach?

Adela Prochyra



Polskie miasta nie różnią się znacząco od miast w innych państwach pod względem podstawowych potrzeb i współczesnych wyzwań, a te przedstawiają się tak, że liczba ludności rośnie, a ilość zasobów, w tym naturalnych, maleje. I trzeba tym zarządzać. Nie zmniejsza się natomiast potrzeba wygody, do jakiej przyzwyczajaliśmy się przez ostatnie dekady. Chcemy żyć komfortowo, a to oznacza wyrażone wprost oczekiwanie użytkowników, że usługi publiczne takie jak transport, administracja, bezpieczeństwo będą na coraz wyższym poziomie. *Smart city* to tylko jedna z opcji rozwiązania tego zagadnienia, urbaniści mówią o różnych jego wariantach: Smart City, Future Smart City, Smart City 3.0 itd. Którą miarą zmierzyć zaawansowanie polskich miast w tej konkurencji? W tym raporcie przedstawiamy pokrótce stan ogólny i miejsce, jakie zajmujemy, na tle innych państw. Trzeba jednocześnie zaznaczyć, że opracowania dotyczące realizacji idei *Smart City* najczęściej liczą kilkaset stron. I jak zaznaczają eksperci, to dopiero początek zmian.

3, 2, 1... Smart City 3.0 – czy to już?

Koncepcja inteligentnego miasta powstała w Stanach Zjednoczonych w latach 60. XX wieku i od tamtego czasu stale ewoluowała. Idee *Smart City* zaczęto wdrażać dopiero na początku XXI wieku. Najpierw (*Smart City 1.0*) impuls pochodził od gigantów sektora usług informatyczno-telekomunikacyjnych, którym zależało głównie na sprzedaży swoich usług, a niekoniecznie na dokładnym dopasowaniu ich do potrzeb mieszkańców miast. W drugiej fazie (*Smart City 2.0*) zamówienia na technologie zaczęli składać przedstawiciele władz lokalnych, którzy poszukiwali pomysłów rozwiązań na poprawę jakości życia mieszkańców. Partnerów i technologie dobierali w bardziej przemysłowy sposób niż poprzednicy. Ta faza jest nadal dominująca, choć coraz częściej mówi się o koncepcji *Smart City 3.0*, która na pierwszym miejscu stawia potrzeby oraz pomysły obywatela i przyjmuje, że nowoczesną technologię wykorzystuje się jako narzędzie do tworzenia lepszych warunków życia w mieście, a nie tylko dla automatyzacji jako takiej. To widać zresztą w rozmowach z przedstawicielami polskich miast. Główna różnica między *Smart City* trzeciej generacji a poprzednimi polega na skupieniu się na inicjatywach mieszkańców. *Smart City 3.0* to podejście, które opiera się na działaniach wszystkich zainteresowanych podmiotów: władz lokalnych, firm i obywateli. Można zaryzykować tezę, że w XXI wieku zarządzanie miastem według założeń *Smart City* stało się koniecznością. Miasta na całym świecie borykają się z wieloma wyzwaniami, takimi jak bezpieczeństwo energetyczne, gospodarka odpadami, zanieczyszczenie środowiska, starzenie się społeczeństw, nierówności społeczne, przeludnienie, ograniczenia w dostępie do surowców, a także z problemami narosłymi w pandemii i nowymi problemami gospodarczymi związanymi z wojną, takimi jak inflacja, ubóstwo czy migracja. Ta złożona mieszanina znanych i całkiem nowych wyzwań sprawia, że życie w miastach staje się coraz trudniejsze, a warunki się pogarszają. Dlatego odporność na te i wiele innych kwestii okazuje się tak istotna

w kontekście ich zdolności do radzenia sobie z niekorzystnymi okolicznościami. Przewiduje się, że do 2040 r. aż 65% światowej populacji będzie żyło w miastach. To oznacza, że wszystkie problemy, z którymi zmagamy się dzisiaj, jeszcze się pogłębią. *Smart city* wydaje się więc sensowną odpowiedzią – łączy wiele dróg, które prowadzą do zrównoważonego rozwoju miast, w których ludzie będą mogli żyć zdrowo, wygodnie i tanio.

Światowy top inteligentnych miast

Zanim dojdziemy do tego, które miasta na świecie są najbardziej *smart*, odpowiedzmy sobie na pytanie, co właściwie sprawia, że miasto jest inteligentne. Większość zaawansowanych pod tym względem graczy łączy jedno – wykorzystują technologię do tego, aby świadczyć mieszkańcom i turystom więcej usług lepszej jakości. Internet przestał być kwestią indywidualnego użytku i wraz z pokrewnymi technologiami

zmienia dziś życie mas i metropolii. Inteligentne miasto nie może obejść się bez technologii i szeregu urządzeń, których działanie oparte jest na tej technologii. Dzięki zastosowaniu unikatowych kombinacji miasta mogą opracowywać systemy do automatyzacji, zarządzania i optymalizacji zasobów. Wśród nich są znane i dość powszechnie dziś wykorzystywane, takie jak czujniki czy sieci bezprzewodowe, Internet rzeczy (IoT), przetwarzanie mobilne, analiza dużej ilości danych (*big data*), *blockchain*, wentylacja grzewcza i klimatyzacja (HVAC), kryminalistyka cyfrowa, systemy sterowania przemysłowego, podłączone i zautomatyzowane pojazdy (CAV), pojazdy elektryczne, recykling pro-

duktów; po rozwiązaniu nieodległej przyszłości: uczenie głębokie (DL), uczenie maszynowe (ML), sieci szóstej generacji (6G), Wi-Fi-7, przemysł 5.0, systemy robotyczne, latające samochody.

Coraz częściej inteligentne miasta podejmują również inicjatywy na rzecz zrównoważonego rozwoju, np. poprzez monitorowanie środowiska, stosowanie urządzeń oszczędzających energię i wodę czy rozwiązań z zakresu energii odnawialnej. Kluczowe obszary, które obejmuje perspektywa *Smart City*, to:

Zielona technologia – ładowanie urządzeń energią słoneczną, bezprzewodowy monitoring, inteligentne kosze na śmieci, zielone budynki, które maksymalizują efektywność energetyczną, pojazdy elektryczne itd.

Zarządzanie ruchem – połączenie czujek, kamer i urządzeń komunikacyjnych wykorzystujących IoT, które ułatwia monitorowanie ruchu i warunków drogowych w czasie rzeczywistym.

Inteligentne sterowanie oświetleniem – takie wykorzystanie czujników, aby uruchamiać oświetlenie tylko wtedy, gdy zbliżają się ludzie lub samochody; oszczędza znaczne ilości energii w porównaniu z tradycyjnymi latarniami ulicznymi.

Woda i ścieki – sprzęt, oprogramowanie, automatyzacja i analiza danych, aby pomóc dostawcom wykrywać i rozwiązywać problemy związane z gospodarką wodną i ściekową.

Bezpieczeństwo – platformy danych, monitoring wideo i urządzenia do wykrywania i zwalczania przestępstw, zwiększające bezpieczeństwo cybernetyczne, a także zapobieganie przestępczości miejskiej.

Reagowanie w sytuacjach kryzysowych – zoptymalizowane wyznaczanie tras w celu szybszego reagowania na sytuacje kryzysowe, kamery CCTV udostępniające nagrania w czasie rzeczywistym centrom obsługi telefonicznej.

Od lat światowe organizacje prowadzą różnego rodzaju rankingi i listy najbardziej inteligentnych miast na świecie. Zwykle do oceny wykorzystuje się w nich kombinację czynników ekonomicznych, kapitału ludzkiego, technologii, zrównoważonego rozwoju, spójności społecznej, transportu, przywództwa i planowania urbanistycznego, innowacyjnego myślenia, wdrażania na dużą skalę technologii inteligentnych miast oraz wizje tych miast dotyczące wykorzystania technologii IoT w celu poprawy życia ich obywateli teraz i w przyszłości. Regularnie na szczycie tych list pojawia się Londyn. Stolica Wielkiej Brytanii liczy ok. 9 mln mieszkańców, a życie w niej jest kosztowne, ale wbrew pozorom świetnie radzi sobie ze współczesnymi wyzwaniami. To jest w dużej mierze kwestią decyzji. Burmistrz Sadiq Khan podjął decyzję, aby uczynić Londyn najbardziej inteligentnym miastem na świecie, i cel ten konsekwentnie realizuje. Ma długofalowy plan. Władze Londynu spodziewają się wzrostu liczby mieszkańców do 11 mln w ciągu kolejnych 25 lat i już się do tego przygotowują. Mapę drogową *Smarter London Together*, określającą projekt rozwoju, zamieszczono na stronie www.london.gov.uk/. Skondensowano go do podania pięciu „misji”: więcej usług zaprojektowanych przez użytkownika, zawarcie nowej umowy na dane miejskie, światowej klasy łączność i inteligentniejsze ulice, wzmocnienie cyfrowego przywództwa i umiejętności oraz usprawnienie współpracy w całym mieście.

Bardzo poważnie są tam traktowane też kwestie ekologii. Miasto ma najniższą emisję CO₂ na mieszkańca spośród wszystkich regionów Wielkiej Brytanii i nadal ogranicza emisję gazów cieplarnianych – cel to zeroemisyjność do 2050 r. Program *Accelerated Green Path* ma wprowadzić 2,2 mln pomp ciepła i zmniejszyć całkowite zapotrzebowanie budynków na ciepło o 40%. Obecnie połowa podróży w obrębie miasta odbywa się pieszo, transportem publicznym bądź rowerem. Do roku 2041 odsetek ten ma wynieść 80%. Ponadto Londyn jest ośrodkiem inteligentnej mobilności, czystych technologii, proptech i govtech, dzięki czemu oferuje duże możliwości rozwoju międzysektorowego.

Warszawa i Wrocław liderami Smart City w Polsce

Jak widać na przykładzie Londynu, można wskazać kilka cech udanego inteligentnego miasta: przewidywanie, analiza danych, ekologia, otwartość i współpraca. Zastosowanie technologii jest niejako tego pochodną. Technologia jest drogą do celu, jakim jest lepsze, bezpieczniejsze, przyjemniejsze i zdrowsze życie we wspólnej przestrzeni.

Przyjrzyjmy się więc, jak te cele są realizowane w Polsce. Jedną z kluczowych miar rozwoju inteligentnych miast jest Indeks CIMI (*Cities in Motion*). Ten złożony projekt prowadzą profesorowie Joan Enric Ricart i Pascual Berrone z Centrum Globalizacji i Strategii IESE w hiszpańskiej Business School wraz z badaczami na całym świecie. Pod uwagę branych jest tam dziewięć kluczowych wskaźników: ekonomia, kapitał ludzki, środowisko,

Ranking inteligentnych miast 2022



Londyn
Wielka Brytania



Nowy Jork
USA



Paryż
Francja



Tokio
Japonia



Berlin
Niemcy

Źródło: IESE Cities in Motion Index 2022
<https://smartcitiesindex.org/>



umiędzynarodowienie, różnorodność społeczna, mobilność i transport, zarządzanie i planowanie rozwoju. Za ich pomocą ocenia się stopień rozwoju 174 miast świata, w tym 79 stolic. W tym prestiżowym rankingu znalazły się jedynie dwa polskie miasta – Warszawa (62. miejsce) i Wrocław (100. miejsce). Warszawa została bardzo wysoko oceniona w kategoriach: administracja (7. miejsce), planowanie przestrzenne (24. miejsce) i transport (26. miejsce), a także w podrankingu *Top 5 European Europe*, w którym zajęła drugie miejsce za Pragę. Wrocław był 11. na 24 uwzględnionych. Które miasta okazały się najbardziej *smart*? Oczywiście Londyn, następnie Nowy Jork, Amsterdam, Paryż, Rejkjavik, Tokio, Singapur, Kopenhaga, Berlin i Wiedeń.

W innym rankingu, przygotowanym przez fDi Intelligence, bardzo dobrze wypadły ponownie Warszawa i Wrocław, a także Kraków i Poznań. Oceniono w nim potencjał 370 „miast przyszłości” na podstawie pięciu kryteriów zbliżonych do stosowanych w CIMI. Polskie miasta doceniono zwłaszcza za przyjazność prowadzenia biznesu. Ponadto Kraków i Wrocław znalazły się w czołówce podrankingu dotyczącego kapitału ludzkiego i stylu życia.

Zatrzymajmy się na moment przy Warszawie, skoro jest to nasze flagowe *smart city*. Program rozwoju stolicy pod nazwą „Strategia #Warszawa2030” jest nieco bardziej zachowawczy niż londyński. Zawiera cztery cele strategiczne: odpowiedzialna wspólnota, wygodna lokalność, funkcjonalna przestrzeń i twórcze środowisko. Wyznacza partnerów wewnętrznych i zewnętrznych oraz biura odpowiedzialne za realizację strategii, określa wskaźniki i ryzyka realizacji. Warszawa nie ma wprawdzie, tak jak Londyn, wyznaczonego *Chief Digital Officer*a, ale zatrudnia p.o. dyrektorkę koordynator ds. przedsiębiorczości i dialogu społecznego. Stanowisko to zajmuje Karolina Zdrodowska, która „zarządza i koordynuje realizacją zadań z zakresu koordynowania polityki gospodarczej i innowacyjnej m.st. Warszawy, realizacji projektów gospodarczych i naukowych przy udziale partnerów prywatnych oraz działalności gospodarczej i zezwoleń, komunikacji społecznej oraz współpracy z organizacjami pozarządowymi”. Ponadto na stanowisko p.o. dyrektora koordynatora ds. zielonej Warszawy powołano Magdalenę Młochowską, która „zarządza i koordynuje realizacją zadań z zakresu ochrony i kształtowania środowiska, rozwoju zieleni oraz ochrony powietrza i polityki klimatycznej”.

Mniejsi gracze: Bolesławiec, Białystok, gmina Ścinawa

Istotą koncepcji *Smart City* jest szczegółowa analiza danych, która pozwala na lepsze zarządzanie zasobami. Przyjrzyjmy się jej na przykładzie oświetlenia, które jest ważne zarówno jeśli chodzi o bezpieczeństwo i komfort mieszkańców, jak i budżet danego miasta czy danej gminy – koncepcja inteligentnego miasta nie kończy się w metropoliach, z powodzeniem stosują ją małe ośrodki.

Lampy palące się całą noc to już przeżytek. Według danych Visual Capitalist oświetlenie uliczne odpowiada za 20% ogólnego zużycia energii w miastach. W wielu polskich miastach wprowadzane są inteligentne systemy oświetleniowe, „podążające” za pieszem, które pozwalają na bardziej efektywne zarządzanie energią. Często sprowadza się to do zainstalowania nowoczesnych systemów oświetleniowych opartych na technologii LED, które wykorzystują światło białe, a więc są bardziej energooszczędne od technologii konwencjonalnej

(lamp rtęciowych i sodowych) i pozwalają na zmniejszenie kosztów eksploatacji nawet do 50–70%! W ramach tych systemów stosuje się inteligentne czujniki, co pozwala na dostosowanie natężenia oświetlenia do aktualnych potrzeb konkretnej przestrzeni. Rozwiązania tego typu są stosowane w wielu polskich miastach – od Warszawy, przez Bolesławiec, nazywany jednym z najbardziej inteligentnych miast w Polsce, po gminę Ścinawę na Śląsku.

Innym zaawansowanym inteligentnym miastem jest Białystok. W tym *smart city* zamiast tradycyjnych biletów komunikacji miejskiej wprowadzono system rejestracji podróży. Aby skorzystać z komunikacji miejskiej, należy zarejestrować swoją kartę płatniczą w systemie Białostockiej Komunikacji Miejskiej i zbliżyć ją przy wejściu do pojazdu i wyjściu z niego. System sam wylicza ofertę najkorzystniejszą dla pasażera, a na koniec dnia sumuje ceny biletów jednorazowych w zależności od strefy. Jeśli ich koszt przekroczy cenę biletu dobowego, to właśnie on zostanie automatycznie przypisany do pasażera. Pieniądże zostaną ściągnięte z konta wieczorem. Niestety, na razie należy samodzielnie wprowadzić ulgi, co wymaga wizyty w punkcie obsługi klienta z dokumentem uprawniającym do bonifikaty. Białystok posiada także jeden z najnowocześniejszych w Polsce zakładów przetwarzania odpadów.

Polski obraz ogólny

Także na rynku monitoringu wizyjnego ściera się stare z nowym – systemy IP powoli wypierają systemy analogowe. Mimo wątpliwości dotyczących inwigilacji obywateli miejski monitoring wizyjny jest stosowany coraz powszechniej, ponieważ znacznie obniża poziom przestępczości. Tak samo jak w przypadku nowinek w transporcie czy oświetleniu, tak i w branży monitoringu pojawiają się nowe rozwiązania, np. zdalny pomiar temperatury ciała, co nie znaczy, że są zawsze skutecznie wykorzystywane. W warszawskiej sieci monitoringu, budowanej od 2001 r., jest obecnie 22 599 kamer, z czego w zintegrowanym monitoringu miejskim zaledwie 486. Lepiej zaplanowano to w Oświęcimiu, gdzie zbudowano zintegrowany nowoczesny system monitoringu bezprzewodowego w technologii CCTV IP. Program Bezpieczne Miasto Oświęcim objął nie tylko centrum miasta, ale także trzy szkoły i przedszkole.

Należy wziąć poprawkę na skalę obu miast. W tych mniejszych często zastosowanie jakiegoś rozwiązania ma większy wpływ niż zastosowanie tego samego rozwiązania w dużym mieście. Największym problemem, który podnoszą specjaliści, jest wybór – czy wdrażanie technologii bez szczegółowego planu. Są miasta, które z racji wielkości nie muszą wprowadzać wielu zaawansowanych rozwiązań, gdyż o podniesieniu jakości życia może zadecydować nawet jedna czy dwie nowoczesne inwestycje, czego przykładem jest ekospalarnia w Tarnowie. Druga problematyczna kwestia to finanse. Najnowocześniejsze technologie, „celowane” w konkretne potrzeby mieszkańców, są drogie. Co prawda są sposoby, aby pozyskać środki na finansowanie nawet bardzo specjalistycznych udogodnień, takich jak system sterowalnej mikroretencji, innowacyjne technologie wzmacniaczy mikrofalowych dla sieci 5G, inteligentne kontrolery lamp ulicznych LED z platformą wspomagającą optymalizację zużycia energii – do czego zachęca m.in. Polska Agencja Rozwoju Przedsiębiorczości (PARP), ale zwłaszcza w tym przypadku potrzeba dobrej współpracy trzech filarów: obywateli, samorządu i biznesu. ●

» Odporność miasta nabiera bezprecedensowego znaczenia, ale może zostać osiągnięta tylko wtedy, gdy wszystkie zainteresowane strony: sektor publiczny, firmy prywatne, organizacje obywatelskie i instytucje akademickie będą współpracować i przyczyniać się do osiągnięcia tego celu. «

Pascual Berrone,
profesor zarządzania strategicznego,
kierownik Katedry Zrównoważonego
Rozwoju i Strategii Biznesowej
Schneider Electric
w IESE Business School



Każde miasto jest inne

Londyn, Nowy Jork, Singapur, Tokio – z tymi miastami najczęściej kojarzy się określenie *smart city*. To metropolie pełne nowoczesnych biurowców i korzystające z technologii, które w Polsce nie są powszechne.

Ale czy rzeczywiście Rzeszów, Lublin albo Kołobrzeg są dalekie od tego, by nazwać je *smart*?

Monika Żuber-Mamak

Przyglądamy się dziś nieoczywistym miejscom na mapie Polski, które w światowych rankingach raczej się nie znajdują, a które wdrażają coraz więcej rozwiązań ułatwiających życie mieszkańcom. Rozmawiamy z ich władzami o strategii rozwoju *smart city*. Gdy pytamy w tym kontekście o bezpieczeństwo, podkreślają, że to dziś tylko jeden z aspektów, i wcale nie najważniejszy, bo nie stanowi wyzwania. Priorytetami są: jakość powietrza i sprawna komunikacja.

Koncepcja inteligentnego miasta została uwzględniona w Krajowej Polityce Miejskiej 2023, która określa działania administracji rządowej związane z polityką miejską w kraju. Ponadto Polski Komitet Normalizacyjny opublikował normę PN-ISO 37120:2015-03 stanowiącą część serii norm ISO dotyczących zrównoważonego rozwoju.

Wiele polskich miast wprowadza liczne rozwiązania *smart*, czyniąc to bez szczególnego rozgłosu. Natomiast uważnie wsłuchują

się w głosy mieszkańców. Nasi rozmówcy, osoby odpowiedzialne za miejskie ulepszenia, wyraźnie ten aspekt podkreślali: wszystko robimy po to, by ludziom żyło się lepiej. Jak powiedział Krzysztof Stańko, pełnomocnik Prezydenta Miasta Rzeszowa, zajmujący się m.in. cyfryzacją kolejnych zadań miasta: *Wszystko, co w Rzeszowie zostało już wykonane, jeśli chodzi o udoskonalenie działania miasta, a także wszystkie projekty dotyczące jego przyszłości, robione jest z myślą o mieszkańcach*. I nie jest w tej opinii odosobniony. Podobne stanowisko przedstawia Artur Szymczyk, zastępca Prezydenta Miasta Lublin ds. Inwestycji i Rozwoju: *Koncepcja smart city w Lublinie jest realizowana od poprzedniego okresu programowania strategicznego, czyli od 2013 r., i jest kontynuowana w ramach nowej Strategii Lublin 2030. Idea smart city przyjęta przez miasto Lublin jest zgodna z paradygmatem „Human Smart Cities 3.0”, w którego ramach mieszkańcy współtworzą miasto, a rola władzy lokalnej skupia się na tworzeniu przestrzeni i możliwości do wykorzystania różnorodnego potencjału obywateli*.



Włodarzom polskich miast, aspirującym do bycia miastami inteligentnymi, nie zależy na tym, by naszpikować przestrzeń technologią. Ani Kołobrzeg, ani Rzeszów nie mają ambicji, by monitorować przestrzeń publiczną tak, jak robi to np. Londyn. Istotą jest uczynienie przestrzeni miejskiej bezpieczną i przyjazną, zapewniającą wygodne życie. Taką, która najlepiej oddaje ideę Human Smart Cities 3.0 przyświecającą choćby Lublinowi.

Najważniejsza jest komunikacja

Od razu wyjaśnijmy – komunikacja w znaczeniu łączność. Rzeszów jest najlepszym przykładem tego, jak wiele w naszym życiu zależy od sprawnej komunikacji.

– Bez sprawnej telekomunikacji nie byłibyśmy w tym miejscu, gdzie jesteśmy. Nasze hasło to Rzeszów stolicą innowacji. I tak jest – przekonuje Krzysztof Stańko. – Zaczęliśmy od telekomunikacji. Sprawna sieć telekomunikacyjna to podstawa, by w ogóle pomyśleć o tworzeniu smart city. Jako pierwsi wprowadziliśmy ogólnodostępną sieć bezprzewodowych punktów dostępowych do Internetu, czyli ResMAN. ResMAN był pierwszy, a proszę pamiętać, że mówimy o początku wieku, kiedy dostęp do Internetu dla wszystkich mieszkańców nie był powszechny – podkreśla z dumą. Odkąd zaczęto szeroko stosować Internet mobilny, sieć ResMAN działa jako sieć wewnętrzna urzędu. W Rzeszowie funkcjonuje 50 km łączy światłowodowych i 20 radiolinii, które zapewniają pokrycie prawie 95% obszaru miasta. Z kolei pasmo radiowe 5G zostało włączone do pracy, zanim ktokolwiek przypuszczał, że będzie wykorzystywane przez telekomunikację.

Do tej sieci są podłączone m.in. kamery miejskiego monitoringu. Również dzięki nim funkcjonuje system zarządzania transportem miejskim. Krzysztof Stańko nie kryje dumy z faktu, że w mieście funkcjonuje system aktywnych tablic elektronicznych na bieżąco informujący pasażerów oczekujących na przystanku. Podobny

funkcjonuje również w Warszawie, podwarszawskim Piasecznie czy we Wrocławiu, Zduńskiej Woli oraz Gorzowie Wielkopolskim. To znacząco ułatwia życie mieszkańcom.

Transport miejski jest również ważny dla Lublina

– Zaplanowane inwestycje dotyczą głównie kwestii mobilności miejskiej oraz elektromobilności. Pierwsze z nich skupiają się na zapewnieniu niezbędnej infrastruktury na potrzeby samochodów elektrycznych. Planowane jest ogłoszenie postępowania przetargowego na wyłonienie operatora i dostawcę stacji. Ma powstać 166 punktów ładowania AC w 83 lokalizacjach, co z istniejącą już infrastrukturą przełoży się na wymagane 210 punktów ładowania w całym mieście – podkreśla Artur Szymczyk, zastępca Prezydenta Miasta Lublina ds. Inwestycji i Rozwoju. – Ważną inwestycją wynikającą z prowadzonej przez miasto polityki transportowej jest budowa Dworca Metropolitalnego. Powstanie nowoczesny węzeł transportowy, którego zadaniem będzie integracja transportu zarówno wewnątrz miasta, jak i komunikacji pozamiejskiej w ramach Lubelskiego Obszaru Metropolitalnego oraz dalekobieżnej.

W obszarze lubelskich projektów miastu udało się m.in. zrealizować system zarządzania ruchem, zmodernizowano transport publiczny w kierunku zeroemisyjnym, uruchomiono szereg rozwiązań w formie e-usług i systemów wspierających transparentność danych publicznych np. geoportala, model 3D miasta czy portal open data.

Zapał i entuzjazm

Te dwa słowa najczęściej pojawiają się podczas dyskusji. Nasi rozmówcy mogliby godzinami opowiadać o tym, co w ich miastach dzieje się nowego, jakie są plany i jak sobie radzą z ewentualnymi trudnościami. Z niezwykłą werwą opowiadała o kołobrzeskich dokonaniach zastępca prezydentki tego miasta Ewa Pelechata,



Polskie inteligentne miasta stawiają na:

- rozwój transportu publicznego
- usprawnienie systemów sterowania ruchem
- monitorowanie zanieczyszczeń
- usprawnienie komunikacji z mieszkańcami
- bezpieczeństwo publiczne
- lepszy dostęp do informacji urzędowych
- ułatwienie uczestniczenia w podejmowaniu decyzji dotyczących projektów realizowanych z budżetu obywatelskiego.

odpowiedzialna za wszystkie inicjatywy smart city. Kołobrzeg jest przykładem tego, że nie od wielkości miasta, a od zaangażowania i zrozumienia idei zależy, czy dana miejscowość zyska nowe funkcje i czy będzie ulepszana.

– Największym problemem są fundusze, ale najważniejsza jest strategia. Mamy wizję rozwoju Kołobrzegu. Najpierw przygotowujemy strategię, później projekty. Na ich bazie pozyskujemy środki w dużej mierze pochodzące z Unii Europejskiej. Mam świadomość, że każde miasto jest inne. Inne będą problemy i potrzeby mieszkańców metropolii, a inne takiego miasta, jakim jest Kołobrzeg. Naszym zadaniem jest dostosować działania do tego, by mieszkańcom żyło się lepiej – przyznaje Ewa Pelechata. To podejście jest szeroko omawiane na stronie i-kolobrzeg.pl.

Co w takim razie Kołobrzeg robi dla mieszkańców? Z rzeczy mało spektakularnych, a bardzo ważnych można wymienić np. robotyzację procesów urzędu. Dzięki temu wzrosła wydajność urzędu miasta, a co za tym idzie sprawy obywateli są załatwiane szybciej. Kołobrzeg prowadzi także mapy ciepła, by sprawdzić, w których miejscach latem temperatura niebezpiecznie wzrasta, by wprowadzić tam zielen. Monitoruje też naturalne tereny retencji i prowadzi systemy informacji transportowej. Te dane są gromadzone w ramach systemu informacji przestrzennej. Na stronie gis.kolobrzeg.pl znajduje się m.in. mapa gospodarki odpadami, plany infrastruktury miejskiej, mapy demograficzne oraz zagrożenia i ryzyka powodziowego. Miasto uruchomiło także kołobrzeską kartę mieszkańca, która zapewnia seniorom bezpłatny przejazd komunikacją miejską, a wszystkim umożliwia skorzystanie z licznych zniżek oferowanych przez firmy partnerskie. Aplikacja Kołobrzeg Re:Generacja, przedstawiająca atrakcje turystyczne miasta, bazę noclegową i gastronomiczną, to tylko wiskienka na cyfrowym torcie.

Podobne sukcesy, jeśli chodzi o usprawnienie obsługi mieszkańców, ma na swoim koncie Łódź, która – jak informuje Biuro Rzecznika: Rozszerzyła katalog usług elektronicznych, w których mieszkańcy i przedsiębiorcy mogą zwracać się do urzędu z wykorzystaniem elektronicznej formy kontaktu. Uwzględniając wszystkie działania związane z aktualizacją usług elektronicznych i udostępnianiem nowych usług online, Urząd Miasta Łodzi na koniec 2022 roku udostępniał łącznie 134 formularze elektroniczne w ramach 99 usług na platformie ePUAP oraz 41 usług na platformie biznes.gov.pl.

Danych wrażliwych nie gromadzimy

Wielu obywateli ma wątpliwości co do tego, jakie dane przekazują do enigmatycznego centrum choćby kamery miejskiego monitoringu. Czy miasto wie, jakie miejsca odwiedzają jego mieszkańcy? Gdzie przebywa konkretny Nowak czy Kowalski? W których sklepach zakupy robi Wiśniewska? Wszyscy nasi rozmówcy wyraźnie zaznaczają, że miejskie systemy monitoringu nie gromadzą danych wrażliwych, choć ilość zbieranych informacji jest olbrzymia.

– Nie prowadzimy rejestru danych. Nie kolekcjonujemy ich. Nie bawimy się w Wielkiego Brata, choć zbieramy sporo informacji. Miejski monitoring służy nam przede wszystkim do tego, by katowiczanom zapewnić większe bezpieczeństwo, dlatego np. gromadzimy informacje dotyczące lokalizacji patroli – mówi Łukasz Żółciak, oficer ds. smart city w katowickim urzędzie, a jednocześnie fan systemu KISMiA (Katowicki Inteligentny System Monitoringu i Analizy). I wyjaśnia, czemu ma służyć to ostatnie działanie: Informacja o lokalizacji patroli policji i straży miejskiej przyczynia się przede wszystkim do optymalizacji pracy tych służb. Kiedy wiemy, gdzie są patrole, wiemy, gdzie może ich zabraknąć.

Systemy miejskiego monitoringu gromadzą przede wszystkim dane dotyczące czystości powietrza. Robią to m.in. Rzeszów, Kołobrzeg, Białystok, Warszawa i co zupełnie zrozumiałe Katowice. Władze Rzeszowa zdecydowały się na instalacje 40 czujek jakości powietrza, a odczyty udostępniają mieszkańcom. Wkrótce mają zostać podłączone czujki na paczkomatach firmy InPost, która umieszcza je tam od dawna w ramach swoich działań związanych ze społeczną odpowiedzialnością biznesu. Po te dane wystarczy tylko się schylić. W Katowicach zbierane są informacje m.in. o zanieczyszczeniu pyłami, wilgotności i poziomie dwutlenku węgla. To ostatnie ma służyć m.in. realizacji założeń uchwały antysmogowej, która od 1 września 2017 r. obowiązuje na terenie województwa śląskiego. Inna rzecz, że miasto, dzięki danym zbieranym przez czujki, może powiadamiać mieszkańców o jakości powietrza danego dnia, choćby po to, by szkoły czy przedszkola mogły w danym rejonie ograniczać wyjście dzieci na „świeże” powietrze.

O jakość powietrza dba także Lublin

– Lubelska Straż Miejska wykorzystuje bezałogowe statki powietrzne (drony) wyposażone w kamery termiczne do badania jakości powietrza. Drony posiadają również mobilny system pomiarowy gazowych

Inteligentne technologie służą do zwiększenia efektywności działania miasta

Dane z czujników oraz zaawansowane centra dowodzenia to nowy sposób zarządzania skomplikowanymi operacjami i automatyzacji systemów infrastrukturalnych. Zmieniło się jednak podejście do rozwiązań cyfrowych. Obecnie to smartfony w rękach mieszkańców są kluczami do miasta, zapewniając szybką informację o transporcie, ruchu drogowym, usługach zdrowotnych, alertach bezpieczeństwa i wiadomościach społecznościowych milionom ludzi. Efektem jest poprawa komfortu życia mieszkańców.

Źródło: Raport grupy roboczej do spraw Internetu rzeczy przy Ministerstwie Cyfryzacji, IoT w polskiej gospodarce





i pyłowych zanieczyszczeń powietrza, który pozwala na kontrolowanie jakości spalania paliw w piecach – wyjaśnia Artur Szymczyk, zastępca Prezydenta Miasta Lublin ds. inwestycji i rozwoju.

Problem z zanieczyszczeniem powietrza ma także Łódź (to niestety bolączka większości polskich miast, o zgrozo także mających często status uzdrowiska). Biuro Rzecznika Prasowego Prezydenta Miasta Łodzi zapewnia jednak, że ta sprawa jest pod kontrolą. I faktycznie, wystarczy wejść na stronę Urzędu Miasta Łódź, by poznać ogólnodostępne dane zbierane z wielu punktów pomiarowych (we współpracy miasta z Veolia Energia Łódź i serwisem Airly) oraz siedmiu ekosłupków. Mieszkańcy korzystający z aplikacji i urządzeń mobilnych mogą zatem na bieżąco sprawdzać stan jakości powietrza.

Partnerska Inicjatywa Miast

Każde miasto jest inne, ale mają podobne problemy: niska jakość powietrza, konieczność usprawnienia ruchu miejskiego, ułatwienie mieszkańcom komunikacji z urzędem, sprawniejsza obsługa transportu publicznego i oczywiście bezpieczeństwo. Osoby zajmujące się realizacją idei *smart city* obserwują uważnie to, co robią inne miasta. W sukurs ma im przyjść Partnerska Inicjatywa Miast (PIM). PIM to, jak czytamy na stronie Ministerstwa Funduszy i Polityki Regionalnej, „program wymiany i promocji wiedzy pomiędzy miastami oraz innymi podmiotami zaangażowanymi w kształtowanie i realizację polityki miejskiej w zakresie prowadzenia przez miasta zintegrowanej polityki miejskiej. PIM jest odpowiedzią na zgłaszaną przez samorządy potrzebę wymiany wiedzy i doświadczeń między miastami oraz innymi podmiotami zaangażowanymi w kształtowanie i realizację polityki miejskiej, a także pozyskiwania pomysłów na wzmocnienie potencjału rozwojowego polskich miast”. Ta szczytna idea ma pewną wadę, czyli niewielki, naszym zdaniem, zasięg. Według oficjalnych informacji w edycji PIM na lata 2021–2023 weźmie udział... zaledwie 30 miast. Zakres tematyczny tej edycji PIM to Miasto Cyfrowe, Miasto Zielone oraz Miasto Inicjatyw Partnerstwa Publiczno-Prywatnego (PPP).

Z PIM pieniędzy jednak nie będzie. W *Zasadach przygotowana i prowadzenia Partnerskiej Inicjatywy Miast w edycji na lata 2021–2023* napisano, iż „obecna edycja PIM nie finansuje w jakiegokolwiek formule (np. grantów) rozwiązań czy projektów opracowanych przez miasta w trakcie jego trwania. Nie wyklucza to jednak łatwiejszego dostępu do finansowania przedsięwzięć ze źródeł zewnętrznych poprzez lepsze przygotowanie odpowiedniej dokumentacji”.

Sieć Miasto cyfrowe	Przykładowe zagadnienia przekrojowe
• Białystok • Dębica • Iława • Lidzbark Warmiński • Łódź • Krzywiń • Piława • Rzeszów • Świdnica • Wyszaków	 budowanie zasobu informacyjnego  integrowanie danych z różnych źródeł  budowa kompetencji cyfrowych  rozwój ekosystemu cyfrowych usług publicznych  uporządkowanie, przetwarzanie i otwieranie danych publicznych

Samymi doświadczeniami trudno jednak wprowadzać innowacje, dlatego tak ciekawy wydaje się funkcjonujący w ramach PIM projekt Miasto Inicjatyw Partnerstwa Publiczno-Prywatnego, czyli takich, które mogłyby pomóc rozwiązać najbardziej prozaiczną przeszkodę – brak pieniędzy. Każdy z naszych rozmówców podkreślał, że nawet najlepsze pomysły giną, gdy nie ma funduszy na ich realizację. Dlatego akurat ten projekt wydaje się tak interesujący. Zważywszy na fakt, że jedna z osób, prosząca jednak w tej kwestii o anonimowość, powiedziała wprost: *Pieniądze by się znalazły w ramach PPP. Są firmy zainteresowane tym, by współpracować z urzędem przy konkretnych projektach. Mielimy np. szansę na uruchomienie profesjonalnego data center, jednak zrezygnowaliśmy. Partnerstwo publiczno-prywatne źle się kojarzy Polakom. Nikt nie lubi być wzywany do sądów.*

Ważne jest jednak, że PIM rozwiązuje inny problem – brak wiedzy, a dokładnie ludzi, którzy rozumieliby, czym jest *smart city* i jak je wdrażać. O tym wspomniała Ewa Pelechata: – *Naszą bolączką jest brak bliskiego ośrodka akademickiego, takiego, z którego do miasta płynęłaby świeża krew. Młodych, pełnych zapału ludzi.* Na to nie mogą narzekać ani Rzeszów, ani Katowice, ani Poznań.

Taka gmina

Należy nadmienić, że władze nie każdego miasta dostrzegają potrzebę unowocześniania. Z przeprowadzonych rozmów wynika, że problem z ewentualnymi innowacjami mają niewielkie miasteczka. Jedna z osób zatrudniona w dziale rozwoju miasta, a w zasadzie miasteczka w zachodniej Polsce, liczącego ok. 10 tys. mieszkańców, powiedziała wprost: *Jakie smart city? U nas to fikcja. Zrobiliśmy aplikację dla mieszkańców, ale nie są nią zainteresowani. Pobrań było tyle, co kot napłakał. Zresztą niby po co mieliby pobierać? Tu prawie wszyscy się znają. Zanim opublikujemy coś w aplikacji lub na stronie urzędu, i tak wszyscy już o tym wiedzą. Chyba nikomu nie zależy. Tu, w urzędzie, wiemy, że sporo polskich miast stara się zyskać status smart city, ale po pierwsze sporo zależy od pieniędzy, a po drugie od... podejścia władz miasta i radnych.*

W podobnym tonie wypowiedział się inny urzędnik z równie niewielkiego miasta, tym razem ze wschodniej części kraju.

CIEKAWY INICJATYWY



Kołobrzeg

Blockchain dla służb uprzywilejowanych – projekt, którego celem jest zminimalizowanie czasu dotarcia i ułatwienie służbom uprzywilejowanym, w szczególności ratowniczym, dostępu do miejsca zdarzenia i osób poszkodowanych oraz zagrożonego mienia. Umożliwi szybkie dotarcie służbom, takim jak pogotowie ratunkowe, straż pożarna, policja, do miejsca zdarzenia, które potencjalnie może wystąpić na terenie zarządzanym przez podmioty biorące udział w projekcie. Dotyczy to szczególnie tych obiektów, które chronione są szlabanami i bramkami. Wdrożona technologia połączy bramy w Kołobrzegu w ekosystem zarządzany za pomocą jednej aplikacji na smartfony, która zostanie udostępniona służbom ratowniczym działającym na terenie miasta.



Lublin

Elektrownia Fotowoltaiczna Hajdów – spółka miejska MPWiK zbudowała elektrownię fotowoltaiczną obsługującą Oczyszczalnię Ścieków Hajdów, by zapewnić efektywność energetyczną. Na obszarze 4 ha zainstalowano 6552 panele monokrystaliczne, osiągające moc szczytową na poziomie ok. 1998,36 kWp. Budowa elektrowni fotowoltaicznej jest kolejnym etapem realizacji strategii MPWiK zakładającej maksymalne wykorzystanie energii własnej. Już od 2000 r. spółka wykorzystuje biogaz, pozyskiwany z fermentacji osadów ściekowych, do produkcji energii elektrycznej i ciepłej. Obecnie z biogazu oczyszczalnia uzyskuje rocznie energię elektryczną na poziomie 10 000 MWh. Po uruchomieniu elektrowni fotowoltaicznej energia ze źródeł własnych zaspokaja ok. 70% ogólnego zapotrzebowania oczyszczalni na energię elektryczną.



Wałbrzych

Inteligentne zarządzanie odpadami – w Miejskim Zakładzie Usług Komunalnych w Wałbrzychu zainstalowano system obejmujący 150 czujników umieszczonych w kontenerach na odpady. Dzięki temu innowacyjnemu projektowi, wykorzystującemu technologię Internetu rzeczy oraz sieć NarrowBand IoT (technologia komunikacyjna oparta na standardzie sieci komórkowych, która została opracowana z myślą o urządzeniach funkcjonujących w ramach IoT), pracownicy MZUK odpowiedzialni za zarządzanie wywozem odpadów mają dostęp do centralnej aplikacji. System umożliwia optymalizację procesu wywozu odpadów komunalnych w Wałbrzychu poprzez regularny pomiar poziomu wypełnienia kontenerów za pomocą czujników ultradźwiękowych działających wiele lat. Dzięki temu rozwiązaniu miasto może zrezygnować z klasycznego harmonogramu wywozu odpadów na rzecz dynamicznego dostosowania wywozu do aktualnych potrzeb i wymagań. Co więcej, dzięki dostępności aplikacji dla użytkownika przez przeglądarkę WWW wdrożenie projektu jest łatwe i nie wymaga dodatkowych inwestycji w infrastrukturę czy sprzęt dla operatorów aplikacji.



Łódź

Pomoc pszczołom – łódzki start-up Intelligent Hives jest twórcą systemu monitorowania, który ułatwia pracę pszczelarzom i pomaga chronić pszczelą populację. Tak zwane inteligentne ule zostały posadowione na terenie Laboratorium Produkcji Ogrodniczej przy Zespole Szkół Rzemiosła. Dzięki specjalistycznym czujnikom i urządzeniom monitorującym możliwe jest poznanie pszczelich zwyczajów, badanie ich stanu zdrowia i aktywności. Dodatkowo w różnych punktach miasta powstają łąki kwietne sprzyjające bioróżnorodności, które dają schronienie i pożywienie pszczołom, a także zatrzymują wodę w gruncie i wpływają na oczyszczanie powietrza oraz obniżanie jego temperatury (mapa na lodz.pl/ekoportal).



Wrocław

SmartFlow, by uniknąć wycieków – wspólnie z firmami informatycznymi Microsoft i Future Processing wrocławskie MPWiK opracowało rozwiązanie, które podzieliło Wrocław na strefy pomiarowe. System informatyczny działa na terenie kilkunastu osiedli mieszkaniowych i wykorzystuje prawie 100 urządzeń do monitorowania ilości i ciśnienia wody przepływającej przez sieć wodociągową. Dzięki temu pracownicy MPWiK mogą łatwo zlokalizować jeden z najtrudniejszych typów awarii wodociągowej, jakim jest tzw. ukryty wyciek. System opiera się na czujnikach rozmieszczonych w sieci, które dostarczają informacje o dystrybucji wody przez całą dobę. Pomiaru są przeprowadzane głównie w nocy. Po wytypowaniu miejsca awarii brygada MPWiK dokładnie je lokalizują, korzystając z rozwiązań akustycznych.



Zakopane

Zdalny odczyt ciepłomierzy – system wdrożony przez PEC Geotermię Podhalańską zapewnia zdalny odczyt ciepłomierzy dokonywany dzięki technologii NB-IoT. System zapewnia spółce Geotermia stały, codzienny dostęp do danych z urządzeń licznikowych zainstalowanych w węzłach sieci ciepłowniczej. To pierwsze w Polsce zastosowanie na potrzeby *smart meteringu* technologii wąskopasmowej LPWAN (Low Power Wide Area Network) działającej w paśmie LTE. Liczniki ciepła często są umieszczane w trudno dostępnych miejscach (np. węzły mediów w piwnicach czy podziemnych pomieszczeniach technicznych), gdzie zasięg standardowej sieci komórkowej nie dociera. Dzięki zastosowaniu LPWAN oraz sensorów wyposażonych jednocześnie w karty SIM umieszczone w ciepłomierzach klient otrzymuje codzienne raporty z każdego miejsca ze skutecznością bliską 100%. Dzięki temu obsługa sieci ciepłowniczej nie wymaga angażowania dodatkowych pracowników, szybsza jest też reakcja na awarie.



– Jakie smart city, kiedy nie mamy pieniędzy, żeby wymienić oświetlenie uliczne na energooszczędne LED-y? Poza tym – dodał konfidencjonalnym tonem – dla tutejszych radnych, a to w ich gestii zależy budżet miasta, to fanaberie. Za taką fanaberię uznali nawet postawienie czujników, które zbierałyby informacje o zanieczyszczeniach. Może i z sensem, przecież zimą gołym okiem widać, że mieszkańcy palą byle czym. Gdyby były na to niepodważalne dowody, to może trzeba byłoby jakoś zareagować? A tak nie ma dowodów, więc nie trzeba nic robić. Chyba musimy poczekać na młodszych ludzi w urzędzie. I młodszych radnych.

Trudno się dziwić, że rozmówcy, którzy wprost przyznali, że w ich miejscowościach nie robi się praktycznie nic, by je unowocześnić, wolą zachować anonimowość, tym bardziej że zawsze pojawia się jeden wątek: problemem nie jest brak pieniędzy (z Unii coś byśmy dostali), a mentalność i niechęć do zmian, które wymagałyby podjęcia jakichkolwiek działań. Jest jak jest, czyli dobrze. Lepiej być nie musi.

Więcej mieszkańców miast?

Jak podaje GUS, pod koniec czerwca 2022 r. ludność Polski liczyła 37 mln 827 tys. mieszkańców. W miastach żyło 22 mln 565 tys. osób, czyli 60% populacji. Z opublikowanego przez GUS podsumowania danych *Ludność. Stan i struktura ludności oraz ruch naturalny w przekroju terytorialnym w 2022 r.* wynika jednak, że wyraźnym trendem jest... malejąca liczba mieszkańców miast. Patrząc jednak na rzecz z dłuższej perspektywy czasowej, widać, że w ciągu ostatnich 10 lat polskim miastom ubyło ok. 3% mieszkańców. Ci ludzie jednak nie zniknęli. Niewielka część z nich wyjechała z kraju, większość zdecydowała się na zamieszkanie na wsi, tyle że owe wsie są przedmieściami wielkich miast. Tak zwana urbanistyka łańcowa kwitnie. Z dużym prawdopodobieństwem można założyć, że niejedna taka miejscowość, stanowiąca w istocie przedmieście dużego miasta, zostanie przez nie wchłonięta przez powiększenie granic administracyjnych (czy ku zadowoleniu mieszkańców to już inna sprawa). Ten problem dobrze przedstawiono w serwisie Kartografia ekstremalna i na mapie przygotowanej przez jej autora Szymona Pifczyka.



NIE KAŻDE MIASTO MUSI BYĆ SMART

ROZMOWA Z DR. TOMASZEM KULISIEWICZEM, WSPÓŁTWÓRCĄ SERWISU INTELIGENTNEMIASTA.PL

Od lat zajmuje się pan ideą inteligentnych miast, zapytam wprost: czy miasta muszą być smart? W jakim celu? Żle nam teraz?

Zdecydowanie nie każde miasto musi być *smart*, jeśli to miałyby oznaczać tylko wdrożenie wielkich systemów informatycznych. Nie zawsze jest taka potrzeba. Natomiast każde miasto, ale i wieś czy miasteczko, powinno być miejscem przyjemnym do życia. Przyjaznym. Nie ma znaczenia, czy naszpikujemy je czujnikami zbierającymi dane, czy nie. Najważniejsze jest, by ludziom żyło się w nim wygodnie, bezpiecznie, dobrze. Lubię koncepcję *citizen as a sensor*, ew. *citizen sensing*. To koncepcja, w której miasto wykorzystuje dane świadomie lub mimowolnie dostarczane przez

Zmiana liczby ludności w latach 2011-2021



Źródło: Kartografia ekstremalna. Zielone obszary wokół największych miast to tysiące nowych domów zbudowanych chaotycznie w ostatniej dekadzie.

Dla miasta oznacza to ni mniej, ni więcej konieczność zaplanowania dróg, mostów, przejazdów, wodociągów, oświetlenia, kanalizacji, szkół i przedszkoli oraz innych elementów składających się na sprawne funkcjonowanie organizmu miejskiego. Z takimi wyzwaniami bez trudu poradzi sobie *smart city*. To odpowiedź na pytanie, po co nam inteligentne miasta, gdyby kogoś naszła wątpliwość.

Pamiętajmy, że nie ma absurdałnych scenariuszy, jedynie nasza wyobraźnia jest zbyt uboga... w przeciwieństwie do wyobraźni hiszpańskich „nurków” poszukujących nocą bursztynu w Bałtyku. ●

mieszkańców, np. pasażerów transportu miejskiego, którzy odbijając karty miejskie w kasownikach, dostarczają tym samym informacji o tym, które linie są bardziej obłożone, a jakimi autobusami nie jeździ nikt. Dzięki temu instytucje odpowiedzialne za funkcjonowanie miasta, wiedzą w jakim rytmie ono żyje. Urzędnicze pomysły nie powstają wówczas w próżni, lecz są odzwierciedleniem potrzeb mieszkańców.

Skoro nie ma potrzeby, by każde miasto było *smart*, to jaka koncepcja dotycząca urbanistyki wydaje się panu obecnie szczególnie ważna lub uznaje ją pan za cenną?

Osobiście cenię ideę miasta 15-minutowego, czyli tak zorganizowanego, że mieszkaniac w zasięgu krótkiego marszu, a raczej spaceru będzie mieć dostępne wszystkie niezbędne mu usługi: szkołę, przychodnię zdrowia, bank, pocztę, sklepy itp. Idealnie byłoby, aby miejsce pracy także znajdowało się blisko.

Istnieje takie miasto idealne?

Nie, nie istnieje. Miała być nim Brasilia, dla której założenia urbanistyczno-architektoniczne opracowali brazylijscy architekci Lucio Costa (plan przestrzenny) i Oscar Niemeyer (budynki użyteczności publicznej). Wiele urbanistów broni Brasilii, ale z różnych powodów ich koncepcja nie do końca się sprawdziła, być może dlatego, że powstała zgodnie z wyobrażeniem architektów, skądinąd znamienitych, lecz rzeczywistość często odstaje od wyobrażeń. Niektóre dawne osiedla, nawet te PRL-owskie osiedla z wielkiej płyty (pomijając jakość budynków) byłyby częścią realizacji tego założenia.

Nowe osiedla rzadko tak wyglądają.

To prawda. Warto pamiętać, że zgodnie z prognozami rośnie migracja do miast, a co za tym idzie, ich rozrastanie się jest zatem nieuniknione. To trend ogólnosiwiatowy i widoczny także w naszym kraju, choć nie na pierwszy rzut oka i nie w przypadku wszystkich polskich miast.

To prawda, piszemy o tym w artykule Każde miasto jest inne, o ile ma pan na myśli urbanistykę łańcową.

Tak, właśnie o niej mówię. Polska cierpi na problem dotyczący planów zagospodarowania przestrzennego, a raczej przejmującego ich braku. W 2017 roku Najwyższa Izba Kontroli opublikowała raport, z którego wynika, że tylko ok. 30% powierzchni kraju pokryte jest takimi planami. Od tego czasu niewiele się zmieniło. Wiele inwestycji mieszkaniowych odbywa się bez planu, chaotycznie. Na dalekich przedmieściach, na terenach odrolnionych powstają, jak je nazywam, „miasta w kapuście”. Już nie wieś, jeszcze nie miasto, a przecież ich mieszkańcy potrzebują dokładnie takiej samej infrastruktury, jak w mieście. Tymczasem gminy, która udostępniła teren, na tę infrastrukturę nie stać.

Wróćmy do smart city. Czy może pan wskazać w Polsce miasto wyjątkowo inteligentne? Czy jakieś pod tym względem się wyróżnia?

Odpowiem tak, jak zazwyczaj odpowiadają prawnicy: to zależy. W tym przypadku zależy, pod jakim względem je rozpatrujemy. Są opracowywane różne rankingi *smart city*. Jest ich wiele, bo każdy uwzględnia inne wskaźniki. Zależy więc, jakie parametry weźmiemy pod uwagę.

To prawda, przygotowując się do rozmowy, trafiłam na bardzo ciekawą pracę Karoliny Ogrodnik, adiunktka na Politechnice Białostockiej, *Multicriteria Analysis of Smart Cities in Poland* opublikowanej w 2020 roku przez „Geographia Polonica”. Autorka przygotowała kilka rankingów uwzględniających różne wskaźniki, m.in. ekonomię miasta, smart mobilność, a nawet wykształcenie mieszkańców.

Właśnie o to chodzi. Na *smart city* należy patrzeć z różnych perspektyw. Chętnie przytaczanym przykładem jest Białystok. Zgadza się, że to miasto ma powody do dumy, jeśli chodzi o modernizację transportu – w tym przypadku w rankingach znajduje się na pierwszym miejscu. Ale we wspomnianym przez panią opracowaniu Białystok zajął dopiero dziewiąte miejsce w kategorii *smart living*, co jednak nie oznacza, że standard życia jest tu niezadowolający, lecz dowodzi, że trudno ująć koncepcję *smart city* w sztywne ramy rankingów i podporządkować ją jakimś wskaźnikom. Warto natomiast obserwować i mierzyć wskaźniki zdefiniowane np. w normie PN-ISO 37120.

Co jest największym wyzwaniem, przed jakim stoją polskie miasta?

Jest nim bezpieczeństwo, ale w innym znaczeniu niż o tym się myśli. Miasta stosują wiele różnych systemów informatycznych działających samodzielnie, w oderwaniu od siebie. Systemy te są niespójne, niepołączone ze sobą, co może stanowić potencjalne źródło sporów kłopotów, pomijając nieprzystawalność interfejsów różnych systemów. Większym zagrożeniem jest to, że próba ich połączenia może prowadzić do powstania luk otwierających hakerom swobodny dostęp do miejskiej infrastruktury.

Inna rzecz, że miasta na całym świecie mają ten sam problem polegający na sformułowaniu dalekosiężnych planów. Bycie *smart city* to moim zdaniem uciekający cel, bo ciągle pojawiają się jakieś inne wyzwanie i nowe technologie.

Rozumiem więc, że nie ma pan ulubionego miasta, ale z pewnością są takie, w których czuje się pan lepiej niż w innych, coś w nich ceni. Lubię Oslo – chyba już 15 lat temu wprowadzono tam opłatę za wjazd do centrum. Hanower ma świetną komunikację publiczną. Bardzo cenię Helsinki – stolica Finlandii ma sporo zalet, jest miastem na ludzką skalę. Natomiast nie przepadam za miejscowościami, w których każdy zaułek jest obserwowany przez kamery monitoringu.

Wiele osób ma obawy dotyczące choćby prywatności związane z monitoringiem wizyjnym. Uważa pan, że słusznie?

Moim zdaniem jak najbardziej słusznie. Wiadomo, że ludzie chcą się czuć bezpiecznie, ale przykład Chin pokazuje, że kamery stanowiące część większego systemu mogą stać się narzędziem opresji. Nie urzędzenia i nadzór powinny dawać nam poczucie bezpieczeństwa, ale budowanie wspólnoty i wzajemne zaufanie.

Tomasz Kulisiewicz – absolwent informatyki Budapeszteńskiego Uniwersytetu Technicznego (1974), doktorat z informatologii na Uniwersytecie Warszawskim (2015). Analityk rynku informatycznego i komunikacji elektronicznej, wykładowca, współpracownik akademickich zespołów badawczych oraz firm analitycznych i doradczych. Autor i współautor publikacji naukowych i raportów analitycznych. Zajmuje się m.in. aspektami społecznymi, gospodarczymi i kulturowymi zastosowań technologii informacyjnych, zagadnieniami usług e-administracji, a także historią informatyki w Europie Środkowej i Wschodniej. Współzałożyciel i ekspert Ośrodka Studiów nad Cyfrowym Państwem. ●



Smart City 4.0

O tym, jak obecnie wdrażana jest idea *smart city* w Polsce, rozmawiamy z ekspertami: dr **Bartoszem Piziakiem** – kierownikiem Laboratorium Innowacji Miejskich URBAN LAB w Instytucie Rozwoju Miast i Regionów, **Wojciechem Łachowskim** – kierownikiem Integratora Danych Miejskich Instytutu Rozwoju Miast i Regionów oraz **Szymonem Ciupą** – dyrektorem ds. strategii w Smart Factor, ekspertem ds. Smart City i GIS.

Michalina Nowak, a&s Polska

Mieszkańcy miast stanowią obecnie ok. 55% światowej populacji, a wg prognoz do 2050 r. ich odsetek wzrośnie do 68%. Ten trend nie ominie też miast polskich, które – jak przewiduje Bank Światowy – do połowy tego stulecia będą zamieszkiwane już przez 70% ludności kraju. Postępująca urbanizacja sprawia, że miasta muszą się mierzyć z długą listą wyzwań dotyczących m.in. smogu i złej jakości powietrza, hałasu, gospodarki odpadami, jakości usług publicznych i zdrowotnych, rozwoju infrastruktury publicznej i komunikacyjnej, zapewnienia bezpieczeństwa, dostępności mieszkań, chaosu przestrzennego, efektywności energetycznej czy nierówności społecznych. Gros tych zadań będzie można realizować dzięki stosowaniu rozwiązań *smart city*.

Inteligentne miasto to cel wielu polskich samorządów. W jego budowie kluczową rolę odgrywają koncepcja i odpowiednia strategia. Polskie miasta zajmują odległe miejsca w światowych rankingach *smart cities* – w większości z nich pod uwagę jest brana tylko Warszawa (wg trzech najpopularniejszych rankingów: IMD-SUTD Smart City Index, Kearney Global Cities Index oraz IESE Cities in Motion Index nasza stolica plasuje się odpowiednio na 75., 64. i 54. miejscu spośród ponad 100 analizowanych ośrodków). W niektórych są uwzględniane również Kraków i Wrocław.

Nie oznacza to, że w Polsce pod tym względem niewiele się dzieje. Certyfikatem *Smart City* mogą pochwalić się również Gdynia, Kielce, Gdańsk i Lublin, a wiele mniejszych miast podąża ich śladem, wprowadzając rozwiązania z zakresu m.in. mobilności, zarządzania zasobami i cyfryzacji.



dr Bartosz Piziak – kierownik Laboratorium Innowacji Miejskich URBAN LAB w Instytucie Rozwoju Miast i Regionów



Szymon Ciupa – dyrektor ds. strategii w Smart Factor, ekspert ds. Smart City i GIS



Wojciech Łachowski – kierownik Integratora Danych Miejskich IRMiR

Gdy mówimy o *smart city*, myślimy zazwyczaj o metropoliach. Czy tylko duże miasta mogą być inteligentne?

Bartosz Piziak (B.P.): Takie mamy skojarzenia, gdyż zazwyczaj na zdjęciach czy grafikach powiązanych z hasłem *smart city* pojawiają się w wyszukiwarkach obrazy rozświetlonych neonami miast, z drapaczami chmur... Brakuje tylko latających dywanów, choć drony już występują. Tak zaczynają wyglądać współczesne azjatyckie metropolie lub budowane za petrodolary miasta na Bliskim Wschodzie. Ale nam nie do końca o to chodzi i na szczęście bycie inteligentnym miastem nie jest zarezerwowane tylko dla tych dużych. Co więcej, moim zdaniem mniejsze miasta w wielu krajach na całym świecie udowadniają, że zmiany w takich ośrodkach mogą być przeprowadzane sprawnie i dynamicznie. Jeśli chodzi o Polskę, wystarczy spojrzeć na różnego rodzaju rankingi, np. poziomu życia, zadowolenia mieszkańców czy nawet przyznawane nagrody *smart*. Okazuje się, że są tam Gdańsk, Wrocław, Gdynia czy Rzeszów, a także mniejsze, np. Leszno, Jaworzno, Kołobrzeg, i zupełnie małe pokroju Pleszewa czy Dusznik-Zdroju.

Trzeba pamiętać, że wszystkie rozwiązania *smart* – czy to technologiczne (te w szczególności), czy społeczne – muszą być odpowiednio dopasowane do danego miasta, jego potrzeb i wyzwań, a wtedy nawet małe ośrodki mogą skutecznie konkurować z największymi. Oczywiście warto zerkać w stronę europejskich liderów w zakresie mądrych rozwiązań miejskich, którymi są od lat takie aglomeracje jak Wiedeń, Oslo, Amsterdam, Kopenhaga czy Barcelona.

Światowe metropolie realizują dziś projekty, o których w Polsce nie słychać, np. Dubaj wdrożył Paperless Strategy i w obiegu urzędowym nie ma już dokumentów drukowanych. Jakie projekty innowacyjne wzorem tych miast zawitają do Polski w najbliższych latach?

B.P.: O Paperless Strategy wdrażanej może wolniej, ale z powodzeniem w firmach działających w Polsce słyszałem już przed co najmniej dwoma laty. Musimy jednak odpowiedzieć sobie na pytanie, do kogo chcemy i powinniśmy się porównywać. Wciąż będę stał na straży tego, że wysoko zaawansowana technologia we wszystkich aspektach naszego życia musi być celem. Wystarczy, że będzie narzędziem, które jest wykorzystywane w coraz większym zakresie, a z roku na rok będzie lepiej. Polska jako kraj, w tym także nasze instytucje państwowe, w ostatnich latach zrobiły duży postęp w zakresie transformacji cyfrowej. Zaskakujący jest tutaj fakt, że najbardziej przyczynił się do tego COVID-19, okazało się bowiem, że w ciągu niespełna dwóch lat przyspieszyliśmy z transformacją cyfrową o prawie pięć lat. Nie musimy być Dubajem Europy, ale już dziś pracujemy nad tym, by udostępniać rozwiązania, które sprawią, że urzędy staną się bardziej przyjazne, więcej spraw będzie można sfinalizować z poziomu systemu ePUAP, a inne usługi cyfrowe będą „podpinane” do istniejących już funkcjonalności. Zwróćmy też uwagę, czy dana sprawa

rzeczywiście wymaga wizyty w urzędzie, bo być może idziemy tam trochę z przyzwyczajenia lub rozpędu.

Jesteśmy więc coraz bliżej cyfryzacji wszystkich bieżących spraw, co kryje się również pod pojęciem *smart city*?

Wojciech Łachowski (W.Ł.): Zdecydowanie tak. W ostatnich latach obserwujemy rozwój aplikacji Mobywatel – widzimy w niej duży potencjał. Podczas niedawnego Forum Miast Małych i Średnich w Chełmie został zaprezentowany plan rozwoju tej apki. Kolejne kroki obejmują włączenie do niej możliwości załatwienia spraw związanych z samorządem lokalnym, m.in. pozyskanie wiadomości na temat podatków, jakie należy uiścić na rzecz miasta, np. podatek od nieruchomości. To ma oczywiście ogromne plusy, bo mamy do czynienia z szybkim przepływem informacji i łatwą obsługą, choć jednocześnie musimy pamiętać, że coraz więcej informacji o nas trafia do „Wielkiego Brata”.

Zatrzymajmy się na chwilę przy danych. Czy polskie miasta wpisują się w trend *open data*?

W.Ł.: Wydaje mi się, że trend *open data* w ostatnim czasie trochę przystopował. Rzeczywiście metropolie, takie jak Warszawa, Trójmiasto, Wrocław, Kielce, udostępniają dużo tego typu danych. W przypadku mniejszych miast wiele zależy od lokalnych liderów. Pozytywnym przykładem są Przemyśl, Siemianowice Śląskie, Legnica – w tych miastach można czerpać korzyści z tego, że dane są otwarte.

Uważam, że ogromny potencjał danych nie jest jeszcze dostatecznie wykorzystywany w miastach. Jest mnóstwo zasobów zgromadzonych w urzędach czy w spółkach

miejskich, które mogłyby zostać udostępnione na potrzeby biznesu czy mieszkańców, ale niestety tak nie jest. Potencjał związany z otwartymi danymi i projekty realizowane w naszym kraju bardzo często nie kończą się sukcesem nie dlatego, że pomysł był zły, ale dlatego że zabrakło w nim wartościowych danych wejściowych.

Rozumiem zatem, że mamy w Polsce barierę związaną z tym tematem?

W.Ł.: Tak, taka bariera występuje, ponieważ te dane trzeba w odpowiedni sposób przygotować, by móc je udostępniać. Poza tym pokazują one również te aspekty, o których władze miasta czasem nie chcą mówić albo wolą pokazać je wybiórczo i z własną „interpretacją”. Otwarcie zbioru to kawa na łąkę. Kolejny aspekt to świadomość tego, jak wiele z takich danych można uzyskać, jakie decyzje na ich podstawie podjąć oraz jakie korzyści dla miasta wyciągnąć. Tego wciąż brakuje. Do największych barier należy jednak niechęć do zmian. W urzędach bardzo często od wielu lat pracują osoby, które są świetnymi specjalistami w swoich dziedzinach, znają się na planowaniu, transporcie, ale wdrażanie pewnych rozwiązań technologicznych budzi w nich lęk. To zjawisko powszechne i według naszych

badan jest to druga największa bariera, po finansach, w zakresie wdrażania nowych rozwiązań technologicznych w samorządach.

Nie możemy jednak bronić się przed *open data* choćby dlatego, że niebawem wejdzie rozporządzenie Parlamentu Europejskiego Data Act, które przewiduje nowe uprawnienia i obowiązki dla szerokiego kręgu podmiotów, w tym dla osób fizycznych, przedsiębiorców oraz sektora publicznego...

W.Ł.: No właśnie, na najbliższe lata Unia Europejska zaplanowała szereg działań zmierzających do zapewnienia możliwości pełnej realizacji potencjału rozwojowego gospodarki z wykorzystaniem danych i uczynienia UE liderem pod względem społeczeństwa opartego na danych. Data Act niejako wymusił w Polsce opracowanie ustawy o otwartych danych i ponownym udostępnianiu informacji sektora publicznego. Samorządy zostaną zobligowane do udostępniania danych na co najmniej czwartym poziomie otwartości, a to oznacza stałe połączenie między aplikacjami opartymi na tych danych a tymi danymi. Skoro dane już są, to należy z nich wyciągnąć jak najwięcej informacji i wniosków. Dzięki przekrojowym analizom zarządcy miast uzyskają holistyczną wiedzę o każdej gałęzi życia miasta i będą mieli podstawę do dalszego planowania.

Co zrobić, aby były one bezpieczne?

W.Ł.: Miasta powinny zastanowić się nad tym, które dane i informacje są szczególnie cenne, i tych danych i informacji należy strzec. Mechanizmy zabezpieczania danych dotyczących miast i innych organizacji są takie same. *Gros* pracy dotyczy właściwej konfiguracji, monitoringu środowisk i odpowiedniej liczby ekspertów.

Jakie są dziś kluczowe wyzwania w obszarze bezpieczeństwa *smart city*?

Szymon Ciupa (Sz.C.): Można je bez problemu wskazać. To m.in. opracowanie odpowiednich polityk oraz procedur związanych z bezpieczeństwem i cyberbezpieczeństwem, rozwój współpracy międzysektorowej, rozwój kompetencji – zarówno w ramach jednostek odpowiadających za bezpieczeństwo, jak i w skali wszystkich komórek miejskich, zabezpieczanie baz danych miejskich przed nieuprawnionym dostępem w oparciu o procedury systemowe, o tym już mówiliśmy. Dochodzi do tego jeszcze rzadko poruszana kwestia, czyli rosnąca luka płacowa pomiędzy sektorem publicznym a prywatnym. To również wpływa pośrednio i bezpośrednio na to, z jakim stopniem rozwoju *smart city* mamy do czynienia w danym mieście.

Problem bezpieczeństwa w polskich miastach od strony technologicznej jest zbyt często ograniczany do monitoringu wizyjnego. To oczywiście ważny komponent, ale nie może być jedyny, zwłaszcza że cały czas spotykamy się z implementacją inteligentnych algorytmów wspierających pracę obserwatorów. Ogromną wartość z punktu widzenia zapewnienia bezpieczeństwa w miastach mają integracja i analiza danych miejskich. Miasta posiadają ogromne zasoby danych, coraz więcej danych zbieramy z wykorzystaniem IoT czy takich technologii jak skanowanie 3D, ale jednostki miejskie wciąż niewystarczająco wymieniają się danymi oraz pracują nad ich ponownym wykorzystywaniem. W znacznym stopniu dotyczy to również komórek odpowiedzialnych za bezpieczeństwo. Bardzo często te jednostki są „biorcami”

» Problem bezpieczeństwa w polskich miastach od strony technologicznej jest zbyt często ograniczany do monitoringu wizyjnego. To oczywiście ważny komponent, ale nie może być jedyny, zwłaszcza że cały czas spotykamy się z implementacją inteligentnych algorytmów wspierających pracę obserwatorów. «

danych – potrzebują różnych informacji od wielu jednostek, ale mają niewystarczającą siłę przebicia.

Zauważalnie jednak rośnie świadomość miast w zakresie konieczności zintegrowanego podejścia do bezpieczeństwa i stosowania technologii dla wsparcia tego obszaru. Wśród kluczowych rozwiązań technologicznych, które cieszą się coraz większą popularnością, są m.in. systemy geoinformatyczne służące integracji i analizie danych, inteligentny monitoring wizyjny, ale również monitoring infrastruktury miejskiej z wykorzystaniem IoT oraz rozwiązania typu *digital twin*, czyli bliźniaki cyfrowe wirtualnie odwzorowujące przestrzeń miejską w 3D (np. ulice), zapewniające możliwości analiz i identyfikacji zagrożeń (np. w różnych obszarach: od bezpieczeństwa ruchu drogowego po infrastrukturę i przestrzeń publiczną).

W.Ł.: Mieszkańcom w Polsce brakuje wiarygodnego źródła informacji, z którego dowiedzą się, gdzie dokładnie na terenie danego miasta jest bezpiecznie, a gdzie nie jest. Na przykład w brytyjskiej policji można dowiedzieć się, w jakim dniu, w jakim okresie, w jakim miejscu i jakie przestępstwa miały miejsce z podziałem na ich kategorie. Co prawda Komenda Główna Policji wdrożyła niedawno mapę zagrożeń bezpieczeństwa, natomiast zakres informacji w nich podawanych oraz ich dokładność lokalizacyjna uniemożliwiają uzyskanie rzetelnych informacji, czy rzeczywiście jest bezpiecznie, czy też nie. Nie ma informacji, czy w danym rejonie notowano np. kradzieże bądź pobicia. Brakuje kluczowych informacji, które mieszkańcy chcieliby uzyskać pomimo rozwiniętych systemów *smart city*.

Kolejna rzecz to rozwiązania, które pomagają w szybkim reagowaniu na różnego rodzaju katastrofy i zagrożenia naturalne. Kiedyś w Polsce nie występowało minitornado. Wraz ze zmianą klimatu niestety takie zjawiska nie należą już do rzadkości. Potrzebne jest więc rozwiązanie, które pozwoli na szybkie uzyskanie niezbędnych informacji i natychmiastowe zareagowanie na zagrożenie. To ogromne pole do zastosowania nowych technologii, aby zoptymalizować zarówno przeciwdziałanie katastrofom naturalnym, jak i usuwanie szkód, jeśli do takich dojdzie.

Kolejną kwestią mającą duże znaczenie jest wykorzystanie rozwiązań do optymalizacji transportu i zarządzania nim, bo to w znacznym stopniu wpływa na bezpieczeństwo mieszkańców. Chodzi o informacje o tym, gdzie i jakie mamy w danej chwili ograniczenia, jak zorganizowany jest ruch, gdzie ulokowane są przejścia dla pieszych – to też można, a wręcz trzeba wspierać z wykorzystaniem analizy danych.

A jeśli chodzi o cyberbezpieczeństwo?

W.Ł.: W tym przypadku niezmiennie „najsłabszym ogniwem” w zakresie cyberbezpieczeństwa w samorządach jest człowiek – brak

świadomości i kompetencji cyfrowych. Szczególnie widoczne jest to w mniejszych miastach, gdzie urzędnicy stosują te same, zazwyczaj proste hasła do różnych systemów informatycznych, które przesyłają kolegom, np. mailem. To dowód braku wyobraźni i podstawowej wiedzy. Bardzo często nie zdają sobie sprawy z tego, jaką wartość mają informacje i dostęp do nich.

Czym, mówiąc najprościej, powinno być inteligentne miasto za 5 czy 10 lat?

B.P.: Nie ma jednoznacznej odpowiedzi na to pytanie. Kiedy myślę o polskim mieście inteligentnym w niedalekiej perspektywie pięciu czy dziesięciu lat, chciałbym, żebyśmy mówili o miastach, w których jeszcze bardziej istotnym ich

elementem jest człowiek. Miasto inteligentne to takie, gdzie mieszkańcom żyje się dobrze. Ważne, aby podejmować działania angażujące różne grupy ludności i wspólnie wypracowywać innowacje społeczne. Nie neguję potrzeb w zakresie nowoczesnych rozwiązań technologicznych, lecz ich zakup i wdrażanie nie powinno być samo w sobie celem nadrzędnym, a jedynie narzędziem przyczyniającym się do podnoszenia jakości życia mieszkańców danego miasta.

Perspektywa pięciu czy dziesięciu lat nie jest odległa. Dostrzegam szybki rozwój technologiczny, np. nasze doświadczenia z OpenAI i czatem GPT. Bez względu na to, czy nadejdzie jakaś „rewolucja”, czy też rozwój polskich smart cities będzie harmonijny, mam nadzieję, że dobrze wykorzystamy ten czas, by żyło się nam lepiej – a więc i oszczędniej, i w lepszym środowisku, i z wykorzystaniem potencjału oraz zaangażowania mieszkańców. ●

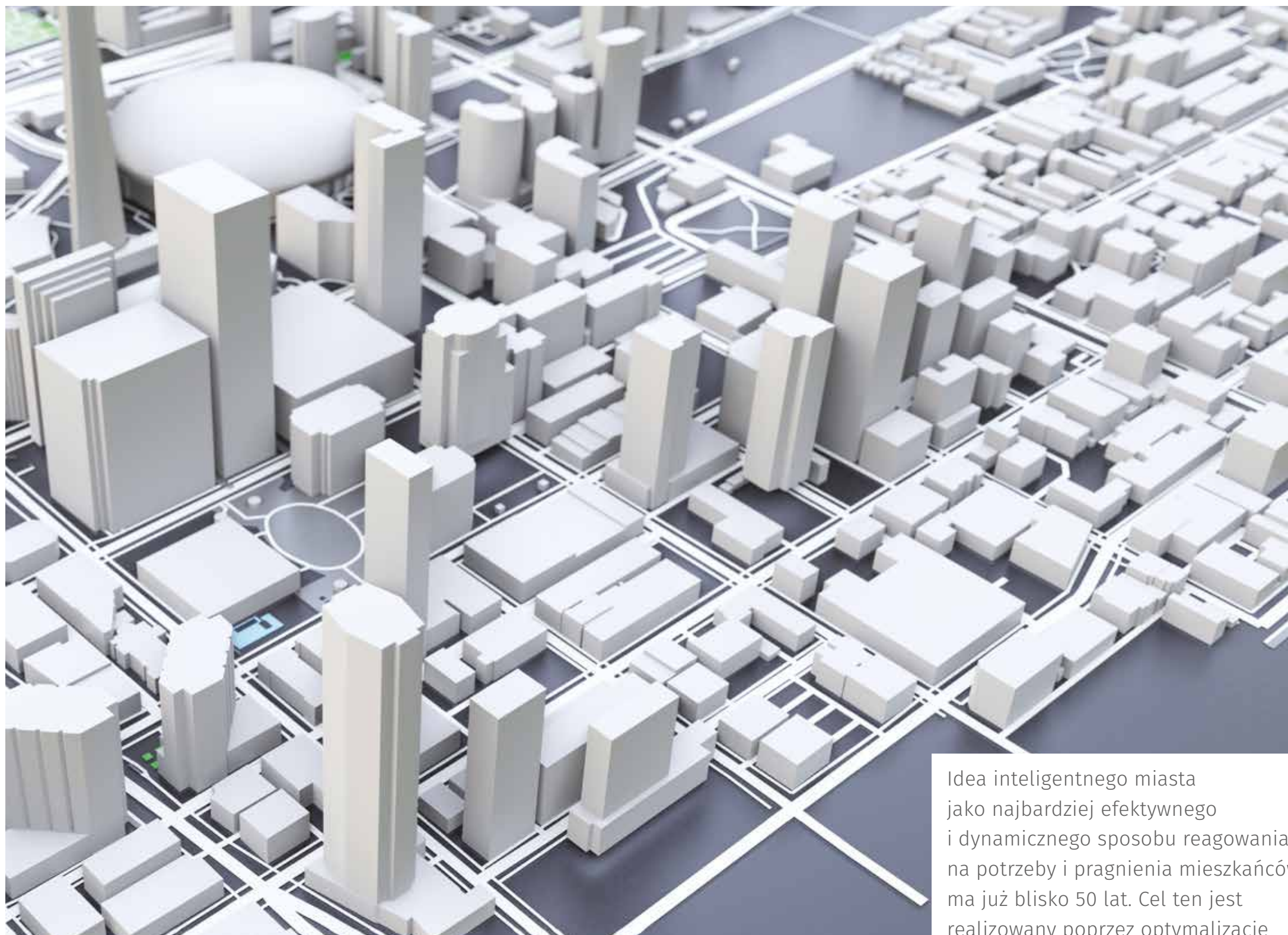
» *Miasto inteligentne to takie, w którym mieszkańcom żyje się dobrze. Ważne, aby podejmować działania angażujące różne grupy ludności i wspólnie wypracowywać innowacje społeczne.* «

RACS 5 v2 Polska platforma kontroli dostępu, bezpieczeństwa i automatyki klasy *Enterprise*

roger
Intelligence for Building

- Obsługa systemów rozproszonych terytorialnie
- Integracja z systemami SSP, SSWiN, CCTV
- Zarządzanie systemami bezpieczeństwa w module VISO SMS
- Integracje z platformami BMS, VMS, SMS, PSIM i aplikacjami do zarządzania biurowcem
- Integracja z usługą Active Directory
- Integracja z serwerowymi systemami windowymi firm KONE, Schindler i innych





Smart city: stara idea w nowej odsłonie

Idea inteligentnego miasta jako najbardziej efektywnego i dynamicznego sposobu reagowania na potrzeby i pragnienia mieszkańców ma już blisko 50 lat. Cel ten jest realizowany poprzez optymalizację infrastruktury, zasobów i przestrzeni z wykorzystaniem błyskawicznie rozwijających się technologii, przede wszystkim cyfrowych.

Jacek Tyburek

P rzełomowym wydarzeniem związanym z ideą inteligentnego miasta był pierwszy kongres *Smart City* w Barcelonie w 2011 roku, gdzie spotkało się kilka tysięcy ludzi z ponad 50 krajów. Firmy technologiczne zaczęły wówczas śmiało pracować nad narzędziami niezbędnymi do tego, by słowo stało się ciałem, a dokładnie idea *smart city* zyskała fizyczny wymiar.

Skomplikowanie charakteryzujące współczesne miejskie organizmy powoduje, że trudno zdefiniować, czym tak naprawdę jest lub powinno być *smart city*. Podawana przez PWN definicja miasta, czyli skupiska ludzkiego, przeciwstawianego wsi, charakteryzującego się zagęszczoną zabudową, zróżnicowaną strukturą społeczną mieszkańców utrzymujących się w większości z zajęć nierolniczych – handlu, rzemiosła, przemysłu i usług, nie przystaje przecież do tego, co już teraz widzimy na własne oczy. Miasto jest przecież zdecydowanie czymś więcej niż tylko ludzkim skupiskiem. Współcześnie to złożone organizmy, funkcjonujące tylko dzięki wsparciu równie złożonej infrastruktury technicznej. Nic więc dziwnego, że przy tak dalekim odejściu od znanej nam tradycyjnej wizji miasta sama koncepcja *smart city* trudna jest do zdefiniowania.

Przez wieki nie zmieniło się natomiast jedno: miasta miały i mają olbrzymią siłę przyciągania. Coraz większa liczba ludzi, rozrastające się przedmieścia, ale też w wielu przypadkach postępująca gentryfikacja powodują konieczność wdrażania nowych rozwiązań, jeśli jakość życia mieszkańców ma mieć choć przyzwoity poziom. Oto kluczowe dziedziny, których rozwój powoduje, że miasto może zasługiwać na miano inteligentnego.

- **Transport miejski:** aktualizacje transportu publicznego w czasie rzeczywistym, inteligentne parkowanie, mikrotransport bazujący na faktycznym zapotrzebowaniu, predykcja konserwacja infrastruktury transportowej i nawigacja drogowa w czasie rzeczywistym.
- **Bezpieczeństwo:** inteligentny nadzór, systemy zabezpieczeń w domu, zarządzanie tłumem, optymalizacja reagowania kryzysowego, mapowanie przestępczości w czasie rzeczywistym oraz kontrole budynków oparte na danych.
- **Opieka zdrowotna:** interwencje w zakresie zdrowia publicznego oparte na danych (takie jak sanitzacja i opieka nad dziećmi), nadzór nad chorobami zakaźnymi, telemedycyna i zdalne monitorowanie pacjentów.
- **Energia:** inteligentne oświetlenie uliczne, systemy automatyki domowej i systemy automatyki dystrybucji.
- **Woda:** monitorowanie jakości wody, śledzenie zużycia wody i inteligentne nawadnianie.
- **Odpady:** optymalizacja systemów zbierania odpadów oraz cyfrowe śledzenie i opłacanie utylizacji odpadów.
- **Rozwój gospodarczy i mieszkalność:** cyfrowe pozwolenia na użytkowanie gruntów i budownictwo, licencje biznesowe, spersonalizowana edukacja, cyfrowe składanie deklaracji podatkowych dla przedsiębiorstw i platformy zakwaterowania typu *peer-to-peer*.

Prymusi *smart city*

Lubimy konkursy i rankingi. Nic więc dziwnego, że powstały też rankingi miast o najbardziej zaawansowanych wdrożeniach systemów *smart city*. Wprawdzie kryteria takich rankingów bywają

niejasne, lecz niezależnie od tego warto poznać listę „najsprytniejszych” miast i wdrożonych przez nie systemów i rozwiązań.

W większości zestawień niekwestionowanym liderem jest miasto-państwo **Singapur**. Projekt Smart Nation miasto rozpoczęło w 2014 roku, wprowadzając m.in. płatności zbliżeniowe w transporcie publicznym, cyfrowy system opieki zdrowotnej, włącznie z wideokonsultacjami oraz urządzeniami typu *wearables* monitorującymi stan zdrowia pacjentów. W 2021 roku władze ogłosiły, że nowe miasto Tengah, położone na zachodzie wyspy, zostanie pozbawione ruchu samochodowego.

Z kolei **Helsinki** za najważniejsze uznały osiągnięcie do 2035 r. neutralności pod względem emisji dwutlenku węgla i wiele wskazuje, że są na dobrej drodze do osiągnięcia celu. Już w 2017 r. miastu udało się obniżyć emisję o 27% w porównaniu z 1990 r. Kolejnym celem, nad którym pracują Helsinki, jest zmniejszenie emisji zanieczyszczeń z ruchu drogowego o 69% do 2035 r. poprzez takie środki, jak przejście całej floty autobusów miejskich na elektryczne oraz rozbudowę metra i sieci ładowania samochodów elektrycznych. Miasto koncentruje się także na wdrażaniu takich rozwiązań, które pozwolą zmniejszyć emisję pochodzącą z budynków o 80% oraz na większym wykorzystaniu energii odnawialnej w budownictwie.

Również **Zurych** i **Oslo** postawiły na zagadnienia ekologiczne jako maszyny napędowe inteligentnego miasta. W Zurychu wszystko zaczęło się od projektu ulicznego oświetlenia. Miasto wprowadziło latarnie, które natężenie światła dostosowywały do natężenia ruchu, co przełożyło się na 70-proc. oszczędność energii. Liczne czujniki rozmieszczone w przestrzeni publicznej dostarczają danych środowiskowych, mierzą natężenie ruchu, ale działają też jako publiczne hot spoty.

Tymczasem już za dwa lata, bo w roku 2025 r., po drogach Oslo mają się poruszać wyłącznie pojazdy z napędem elektrycznym. Miasto zadbało o stosowne udogodnienia dla ich posiadaczy, w tym bezpłatne parkowanie, możliwość korzystania z buspasów, niższe podatki i opłaty za przejazd. Oslo również chce osiągnąć zerową emisję CO₂ i daje sobie na to czas do roku 2030. Z tego też powodu nowe budynki mają być zeroemisyjne do 2030, a te już istniejące należy zmodernizować pod tym kątem do 2050 r.

Jednym z najbardziej scyfryzowanych miast jest jednak **Amsterdam**. Projekt inteligentnego Amsterdamu rozpoczął się w 2009 r. i obejmuje ponad 170 różnych operacji w całym mieście. To, co wyróżnia to miasto, to jego zdolność do pozostania innowacyjnym, niezależnie od tego, czy chodzi o wykorzystanie energii odnawialnej do elektrycznych śmieciarek, instalację zasilanych energią słoneczną przystanków autobusowych, billboardów i światel, czy też budowę pływającej wioski Schoonship powstałej w miejscu, które wcześniej było jedną z najbardziej uprzemysłowionych części Amsterdamu. W całym mieście tysiące budynków zostało zmodernizowanych z zastosowaniem energooszczędnej izolacji dachów, automatycznej regulacji natężenia światła, inteligentnych liczników i energooszczędnych diod LED.

Nowy Jork, od dawna zmagający się z kwestią bezpieczeństwa mieszkańców, może pochwalić się największym zagęszczeniem kamer w USA – na każdy kilometr kwadratowy w 2020 r. przypadało prawie 26 kamer. Setki inteligentnych czujników rozmieszczono w różnych dzielnicach Nowego Jorku w ramach programu pilotażowego inteligentnych miast w 2020 r. Program gromadzi dane, aby pomóc w wydajniejszym zarządzaniu usługami, takimi jak gospodarka odpadami i zbiórka. W mieście zamiast budek telefonicznych pojawiły się również inteligentne huby z technologią zbliżeniową, Wi-Fi oraz stacjami ładowania online. Usługi współdzielenia samochodów są również bardzo popularne w Wielkim Jabłku, co przyczynia się do zmniejszenia emisji spalin i korków.

Aby zachęcić mieszkańców do kreatywności, w mieście organizuje się każdego roku konkurs – z wysoką nagrodą pieniężną – wyłaniający aplikacje, które najlepiej wykorzystują otwarte zbiory danych miasta.

Jednym z najbardziej spektakularnych przykładów jest **Songdo**, nowoczesne miasto biznesowe, powstałe na sztucznie usypanej wyspie w pobliżu miasta Incheon w Korei Południowej, stanowiące część Specjalnej Strefy Ekonomicznej Incheon. Dane są sercem projektów inteligentnych miast w **Seulu**. Poprzez gromadzenie i analizę wzorców miejskich, takich jak przepływ ruchu, prędkość i jakość powietrza mierzona przez czujniki i CCTV rozmieszczone w całym mieście,

tworzą solidną podstawę inteligentnej infrastruktury i usług. Koncentrując technologię na starzejącej się populacji miasta, uruchomiono inicjatywę bezpieczeństwa na rzecz samotnych seniorów. Gdy przez określony czas nie zostanie wykryty żaden ruch lub jeśli czujniki środowiskowe wykryją nienormalną temperaturę, wilgotność lub oświetlenie, natychmiast skontaktują się z odpowiednimi pracownikami prowadzącymi sprawę i służbami ratunkowymi. Również Seul rozważa wykorzystanie platformy danych do stworzenia detektywa AI do oznaczania potencjalnych wzorców przestępczości. Obecnie dzięki sieci 5G stolica Korei jest także jednym z pierwszych miast, które wykorzystują technologię 5G w mobilności i transporcie.

Gdzie w smart city miejsce dla tradycyjnego security?

W zmieniającym się rozumieniu potrzeb i wyzwań security na pierwszy plan wysuwają się zagadnienia zapewnienia prywatności, bezpieczeństwa danych, cyberbezpieczeństwa oraz zapobiegania cyberprzestępczości.

Większość ludzi chciałaby czerpać profity z faktu mieszkania w *smart city*, ciesząc się bezpieczeństwem, wygodą i lepszą niż w miastach tradycyjnych jakością życia. Ma to jednak cenę – kamery monitorujące zainstalowane w każdym zakątku miasta mogą zapobiegać przekraczaniu prędkości i innym wykroczeniom, ale świadomość, że „Wielki Brat patrzy” może być niepokojąca.

Wyzwania związane z bezpieczeństwem są powodem, dla którego wiele osób podchodzi sceptycznie do projektów inteligentnych miast. Każde miejskie urządzenie IoT może stanowić potencjalną

lukę w zabezpieczeniach. Rosnąca liczba czujników IoT i zwiększona łączność wzajemnie zależnych silosów infrastruktury miejskiej budzi uzasadnione obawy. Jeśli standardy bezpieczeństwa pozostaną niezmienione, pewnego dnia cyberprzestępcy mogą unieruchomić całe miasto.

Na szczęście firmy technologiczne tworzą rozwiązania dla inteligentnych miast oparte na analizie dużych zbiorów danych, *block-chaine* i szyfrowanie, które są zaprojektowane do zapobiegania cyberatakami. Deweloperzy inteligentnych miast inwestują w systemy bezpieczeństwa nowej generacji, aby eliminować zagrożenia.

W raporcie *Global Risks 2020* opracowanym przez Światowe Forum Ekonomiczne cyberataki zostały uznane za jedno z najważniejszych zagrożeń globalnych. W tej kategorii znajdują się m.in. kradzież danych, ataki *ransomware*, przejęcie kontroli nad infrastrukturą IT. W niniejszym raporcie stwierdza się ponadto, że ryzyko jest większe w przypadku technologii, które rozciągają się na świat fizyczny, w którym funkcjonują hybrydowe systemy cyfrowo-fizyczne, jak ma to miejsce w przypadku inteligentnych miast. Ataki te oznaczają nie tylko poważne konsekwencje dla mieszkańców miast, ponieważ skuteczny atak mógłby sparaliżować inteligentne miasta, ale także znaczny koszt. Swego czasu IBM obliczył, że średni koszt wycieku danych wynosi ok. 3,92 mln dolarów.

Bezpieczeństwo *smart city* jest zatem jednym z priorytetów przy wdrażaniu tego nowego modelu miasta. Co więcej, to właśnie wzajemna łączność charakteryzuje inteligentne miasta, co zwielokrotnia ryzyko, na jakie naraża się miasto, jeśli nie wdraża proaktywnie programów inteligentnego bezpieczeństwa.

Dla branży security smart city zaczyna się od konstrukcji budynku

Inteligentny budynek to taki, który wykorzystuje cyfrowe narzędzia (czujniki i oprogramowanie) do obsługi budynku, w tym oświetlenia, sprzętu przetwarzającego, hydrauliki, systemów kontroli dostępu, oznakowania cyfrowego, wyszukiwania drogi i systemów zabezpieczeń.

Jednym z najbardziej zaawansowanych technologicznie budynków jest The Edge w Amsterdamie. Według agencji Bloomberg, The Edge jest najbardziej inteligentnym i najbardziej ekologicznym budynkiem na świecie. Otrzymał najwyższą ocenę pod względem zrównoważonego rozwoju, jaką kiedykolwiek przyznano: 98,4%. Wewnątrz znajduje się ok. 28 tys. czujników służących do sterowania wszystkimi instalacjami, ale umożliwiającymi też obsługę osób znajdujących się w budynku.

Gmachy takie jak The Edge będą wyznaczać rozwój budynków inteligentnych, które wpłyną na rozwój *smart cities*. To trend nieunikniony, gdyż Organizacja Narodów Zjednoczonych przewiduje, że do roku 2050 dwie trzecie światowej populacji będzie mieszkać w miastach. Te stają się niezwykle złożonymi ekosystemami społecznymi i technologicznymi. Zarządzanie nimi już jest swoistym egzaminem, a wiele wskazuje, że wyzwania, przed jakimi stoi ludzkość, takie jak zmiany klimatu i problemy demograficzne, uczynią to zadanie jeszcze bardziej skomplikowanym. Dlatego tak wiele państw dąży do tego, by przynajmniej ich metropolie, tradycyjnie przyciągające największą liczbę mieszkańców, były coraz bardziej inteligentne, prowadząc transformację w kierunku miejsc coraz bardziej przyjaznych ludziom. ●

Inteligentne aplikacje które będą istotne dla miast do 2025 r.:

- Mapowanie przestępczości w czasie rzeczywistym
- Wykrywanie strażaków z broni palnej
- Inteligentny monitoring wizyjny
- Reagowanie w sytuacjach kryzysowych
- Kamery nasobne
- Systemy wczesnego ostrzegania o katastrofach
- Aplikacje ostrzegawcze na smartfony
- Systemy sygnalizacji włamania
- Inspekcje budynków oparte na danych
- Zarządzanie tłumem

Źródło: Raport Smart Cities: Digital Solutions for a More Livable Future, McKinsey & Company



Jacek Tyburek

Menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa: od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia Organisational Resilience. Obecnie związany z Black Onion Resilience Community.



Inwestycje w monitoring miejski pozwalają zmniejszyć liczbę niebezpiecznych zaułków

Rozbite butelki na boisku szkolnym, zniszczone elementy placu zabaw czy zakorkowana droga i brak możliwości przejazdu karetki – to codzienność w polskich miastach. Regularne patrole policji i strażników miejskich oraz inwestycje w nowoczesne technologie, takie jak monitoring wizyjny, pozwalają ograniczyć akty wandalizmu oraz inne nieodpowiednie zachowania obywateli.

Jak wynika z raportów poszczególnych jednostek straży miejskiej i policji, w zależności od wielkości miasta codziennie jest przyjmowanych od kilkudziesięciu do nawet 2 tys. zgłoszeń z prośbą o interwencję. Często jedynie połowa z nich przekłada się na liczbę realnych działań. Wiele niebezpiecznych dla mienia, a nawet życia mieszkańców zachowań można ograniczyć dzięki zastosowaniu nowoczesnych rozwiązań w systemach monitoringu wizyjnego z analizą obrazu, dźwięku i danych.

– Z raportów służb porządkowych wynika także, że znaczna część zgłoszeń z prośbą o interwencję dotyczy przestrzeni publicznych, najczęściej terenów parków miejskich, a nawet placów zabaw. Dokładnie taki sam obraz niebezpiecznych miejsc wyłania się ze zgłoszeń, które przyjęliśmy w ramach zorganizowanego przez nas konkursu „Bezpieczny zaułek”. Miasta i gminy z całej Polski przesłały aż 37 zgłoszeń – mówi Konrad Badowski z Axis Communications.

Firma Axis Communications zaprosiła do konkursu „Bezpieczny zaułek” gminy miejskie i miejsko-wiejskie, łącznie aż 96 jednostek terytorialnych. Gminy mogły zgłosić miejsca charakteryzujące się podwyższonym poziomem zagrożenia bezpieczeństwa publicznego lub wysokim wskaźnikiem antyspóecznych zachowań, które w ich opinii wymagają wzmożonej ochrony. Osoby zgłaszające niebezpieczne zaułki miały do wyboru jedną z dziewięciu konkursowych

BEZPIECZNY

ZAUŁEK



kategorii – od zagrożeń związanych z czynnikami zewnętrznymi, zagrożeń związanych ze wzmożonym ruchem drogowym po czynniki zagrażające środowisku i zdrowiu mieszkańców. Zdecydowana większość wszystkich projektów dotyczyła zagrożeń w przestrzeni publicznej – na poszczególnych ulicach miast, na placach zabaw, boiskach szkolnych i w parkach miejskich.

Jury konkursu, złożone z ekspertów do spraw bezpieczeństwa, smart city oraz przedstawicieli organizacji samorządu terytorialnego, oceniło każde zgłoszenie według czterech kryteriów:

- społecznych korzyści z rozwiązania problemu – dla zdrowia, życia czy mienia mieszkańców;
- skuteczności – na ile instalacja gwarantowana zwycięzcy konkursu zapewni bezpieczeństwo w danym miejscu;
- możliwości zastosowania inteligentnych rozwiązań Axis w danym miejscu;
- dotychczasowej działalności gminy/jednostki pomocniczej w celu rozwiązania problemu bezpieczeństwa we wskazanym miejscu.

– Celem konkursu było wytypowanie problematycznych miejsc i pokazanie, że można zadbać o ich bezpieczeństwo w prosty i bardziej efektywny sposób. Każda kamera, głośnik czy czujnik uruchamiający komunikat dźwiękowy przyczyniają się do powstania

kolejnego bezpieczniejszego miejsca więcej. Miasta, widząc potencjał tych rozwiązań, zgłosiły konkretne lokalizacje, w których z powodzeniem można zastosować poszczególne elementy systemu monitoringu miejskiego, aby następnie w pełni kontrolować bezpieczeństwo w tych miejscach. Ze wstępnych analiz konkursu wynika, iż najbardziej potrzebnym rozwiązaniem okazują się kamery z analityką wizyjną, która umożliwia np. wykrywanie zdarzeń niepożądanych – dodaje Konrad Badowski.

Bezpieczeństwo jest jedną z głównych potrzeb człowieka. Władze miast wstępują się w tę potrzebę i wykorzystują możliwości nowoczesnych rozwiązań monitoringu wizyjnego dla zwiększania bezpieczeństwa, a tym samym podniesienia komfortu życia swoich mieszkańców. Spośród zgłoszonych 37 lokalizacji jury konkursu wybrało zwycięskie miejsce, dla którego zostanie zaprojektowane i zrealizowane indywidualne, inteligentne rozwiązanie bezpieczeństwa. Gratulujemy Pabianicom, ich projekt bezpiecznego boiska wybrano. ●



Axis Communications Poland
ul. Domaniewska 44 bud. 4
02-672 Warszawa
www.axis.com/pl-pl/



Hikvision wspiera Smart City 3.0



Miasta na całym świecie wykorzystują zaawansowane technologie, aby poprawić jakość życia mieszkańców. Najnowsza iteracja rozwoju inteligentnych miast, Smart City 3.0, skupia się na tworzeniu bezpiecznych i bezproblemowych środowisk miejskich. Dzięki szerokiej gamie produktów i rozwiązań Hikvision, wiodący dostawca produktów dozoru wizyjnego i zabezpieczeń, jest dobrze przygotowany do wspierania rozwoju inicjatyw Smart City 3.0.

Michał Swoboda

Jednym z kluczowych wyzwań stojących przed władzami miast jest zapewnienie bezpieczeństwa ich mieszkańcom. Kamery PTZ (*Pan-Tilt-Zoom*) i technologie ANPR (*Automatic Number Plate Recognition*) firmy Hikvision zostały zaprojektowane z myślą o tym wyzwaniu, zapewniając możliwość monitorowania i wykrywania zdarzeń w czasie rzeczywistym.

Najnowsze kamery PTZ TandemVU zostały wyposażone w obiektyw z 36-krotnym zoomem optycznym oraz przetwornik 1/1.8" CMOS ze skanowaniem progresywnym, który umożliwia przechwytywanie

wysokiej jakości obrazu nawet w warunkach słabego oświetlenia (technologia DarkFighter). Kamery mają również wbudowany oświetlacz IR (podczerwieni) o zasięgu do 500 m, dzięki czemu idealnie nadają się do pracy na dużych obszarach.

Kamery TandemVU są wyposażone również w zaawansowane funkcje inteligentne, takie jak rozpoznawanie twarzy i śledzenie obiektów, umożliwiając wykrywanie w czasie rzeczywistym potencjalnych zagrożeń. Można je zaprogramować tak, aby automatycznie śledziły określony obiekt lub osobę, a także wysyłały alerty do pracowników ochrony w przypadku wykrycia nietypowych zachowań. Dzięki temu możliwe jest szybkie reagowanie na incydenty związane z bezpieczeństwem i minimalizowanie ryzyka wyrządzenia szkody mieszkańcom.

Kolejnym ważnym aspektem Smart City 3.0 jest potrzeba stworzenia płynnego systemu ruchu miejskiego, który będzie wolny od korków i opóźnień. Rozwiązania ITS (*Intelligent Transportation System*) firmy Hikvision zostały zaprojektowane tak, aby pomóc miastom osiągnąć ten cel, zapewniając zaawansowane możliwości monitorowania i zarządzania ruchem. Kamery 4K ColorVu idealnie nadają się do monitoringu ruchu drogowego dzięki obrazowi wysokiej jakości i możliwości pracy przy słabym oświetleniu, co zawdzięcza technologii ColorVu.

Technologie ANPR firmy Hikvision, wykorzystujące wsparcie radarów mikrofalowych, są krytycznie ważnymi elementami

rozwiązań ITS. Umożliwiają automatyczne rozpoznawanie tablic rejestracyjnych, co znajduje zastosowanie przy pobieraniu opłat, zarządzaniu parkowaniem i kierowaniu ruchem. Kamery i radary mogą być używane w połączeniu z oprogramowaniem do zarządzania materiałem wizyjnym Hikvision, które zapewnia monitorowanie i analizę danych dotyczących przepływu ruchu w czasie rzeczywistym. Dzięki temu miasta mogą zoptymalizować ruch na najbardziej zatłoczonych arteriach, zmniejszyć zatory i zwiększyć bezpieczeństwo na drogach.

Oprócz kamer PTZ, technologii ANPR i rozwiązań ITS, Hikvision oferuje również wiele innych produktów i rozwiązań wspierających ideę Smart City 3.0. Przykładowo technologia Hikvision AcuSense została zaprojektowana w celu zmniejszenia liczby fałszywych alarmów dzięki dokładnemu wykrywaniu wtargnięć ludzi i pojazdów. AcuSense może być stosowane w połączeniu z oprogramowaniem do zarządzania materiałem wizyjnym, które umożliwia monitorowanie i alarmowanie w czasie rzeczywistym.

Hikvision oferuje również szereg rozwiązań kontroli dostępu, które są krytyczne dla zapewnienia bezpieczeństwa budynków i przestrzeni publicznych. Rozwiązania te obejmują technologie rozpoznawania odcisków palców, rozpoznawania twarzy oraz RFID (*radio-frequency identification*), które mogą być wykorzystywane do kontroli dostępu, śledzenia czasu pracy oraz zarządzania gośćmi.

Jedną z kluczowych zalet Smart City 3.0 jest możliwość wykorzystania zaawansowanych funkcji AI w celu poprawy bezpieczeństwa i wydajności zarządzania miastem. Produkty Hikvision zawierają wiele funkcji AI, w tym rozpoznawanie twarzy, wykrywanie obiektów i analizę zachowania. Funkcje te mogą być wykorzystane do identyfikacji podejrzanych zachowań, śledzenia ruchu osób lub pojazdów, a nawet wczesnego ostrzeżenia o potencjalnych zagrożeniach.

Smart City 3.0 reprezentuje nową erę rozwoju miast, w której miasta wykorzystują zaawansowane technologie do tworzenia bezpiecznych, wydajnych i zrównoważonych środowisk miejskich. Rozwiązania Hikvision wpisują się w tę ideę, oferując szereg innowacyjnych rozwiązań zaprojektowanych w celu poprawy bezpieczeństwa pieszych, łatwości wykrywania przestępców i wielu zaawansowanych funkcji AI. Dzięki temu technologie miasta mogą tworzyć bezpieczniejsze, bardziej wydajne i przyjazne środowisko życia dla mieszkańców. ●



Hikvision Poland
ul. Żwirki i Wigury 16B, 02-092 Warszawa
michal.swoboda@hikvision.com
<https://www.hikvision.com/europe/>



SPIN AI – wsparcie dla inteligentnych systemów monitoringu w miastach

Rosnąca świadomość miast i gmin dotycząca rozwiązań typu *smart city* powoduje, że coraz więcej uwagi poświęca się możliwości wykorzystania sztucznej inteligencji w celu automatyzacji i optymalizacji różnorodnych procesów. Jednym z systemów z tego obszaru, które mają szansę zrewolucjonizować m.in. miejski monitoring wizyjny oraz środowiskowy, jest SPIN AI. Warto przyjrzeć mu się również dlatego, że promuje – nieśmiało wciąż omawianą – ideę „AI dla każdego”.

Pomysł na system SPIN AI pojawił się w 2019 r., a impulsem do jego wdrożenia stał się rozwijany przez gdańską firmę OKE Poland system Civileo Smart City, który wykorzystuje algorytmy sztucznej inteligencji do automatycznej analizy przestrzeni miejskich.

System Civileo wykrywa obiekty i analizuje zdarzenia w czasie rzeczywistym na podstawie danych zbieranych z różnych źródeł – kamer dozorowych, mikrofonów i czujników. Dzięki zastosowaniu AI umożliwia nie tylko reagowanie na bieżąco na sytuacje awaryjne

i niepożądane, ale także zapobieganie im dzięki predykcji. Użytkownicy i dostawcy takich systemów wiedzą, że utrzymanie skutecznych funkcji analitycznych może być jednak czasochłonne i kosztowne. W szczególności zmieniające się warunki, np. związane ze zmianą pór roku w monitorowanym obszarze czy zjawisko znane jako dryft koncepcji analityk, często skutkują obniżeniem jakości danych, powodując konieczność douczania modeli AI.

SPIN AI znacząco przyspiesza i usprawnia te procesy, pozwalając na osiągnięcie znacznej oszczędności czasu i kosztów wdrożenia oraz utrzymania systemów opartych na uczeniu maszynowym. Automatyzuje bowiem nie tylko proces zbierania danych oraz ich adnotacji, ale również zarządzanie modelami sieci neuronowych. Tego rodzaju wsparcie jest obecnie kluczowe dla szerokiego spektrum aplikacji IoT w obszarze *smart city*.

Warto zauważyć, że dzięki elastyczności SPIN AI przyczynia się do usprawnienia procesu kontroli jakości analityk poprzez umożliwienie szybkiej walidacji jakości detektorów dla nowych czy istniejących lokalizacji. Moduł statystyk modeli umożliwia porównywanie i dobieranie najlepszych rozwiązań dla konkretnych przypadków.

Dla twórców SPIN AI istotnym elementem tworzenia systemu było też propagowanie idei „AI dla każdego”. Daje on możliwość stosowania zaawansowanych algorytmów

sztucznej inteligencji przy jednoczesnym wyeliminowaniu konieczności zatrudniania wyspecjalizowanej kadry.

Mimo że system ewoluował z potrzeb branży *smart city*, spektrum jego zastosowań jest znacznie szersze. Może on operować na danych ze zróżnicowanych źródeł nie tylko wizyjnych czy dźwiękowych, ale również tych o specyficznych formatach i wymagających dużej precyzji oznaczania, np. danych medycznych. Dodatkowymi atutami są prostota i elastyczność, które sprawiają, że system jest idealnym rozwiązaniem dla wielu branż, ponieważ umożliwia automatyzację powtarzalnych żmudnych zadań.

Sztuczna inteligencja ma szansę stać się użytecznym i prostym w obsłudze narzędziem, które odciąży użytkowników skomplikowanych systemów, dając im jednocześnie możliwość pełnego dostosowania ich do specyficznych potrzeb.

W miarę jak coraz więcej miast będzie podążać w kierunku bycia *smart* – a nawet więcej – *wise*, dzięki świadomości potrzeb swoich mieszkańców, rozwiązania takie jak SPIN AI staną się kluczowe dla realizacji wizji inteligentnych, efektywnych i zrównoważonych przestrzeni miejskich. ●



OKE Poland
ul. Jana Heweliusza 11, 80-890 Gdańsk
<https://oke.pl/>
office@oke.pl



Lidar w projektach *smart city* – najważniejsze korzyści z zastosowania

Lidar to najnowocześniejsza technologia zyskująca w ostatnim czasie popularność. Znajduje zastosowanie przede wszystkim w pojazdach autonomicznych, ale może być również wykorzystywana w miastach, by stały się inteligentnymi.

William Pao, asmag.com

Nazwa lidar jest skrótem od *light detection and ranging*, czyli sposobu pomiaru odległości poprzez oświetlenie celu światłem laserowym i pomiar odbicia za pomocą czujnika. Różnice w czasie powrotu wiązki lasera oraz zmiana długości fali służą do stworzenia trójwymiarowego modelu „oświetlanego” laserem obiektu.

Czujnik lidarowy emituje impulsy laserowe, które napotykając na obiekty, tworzą szczegółową mapę 3D otoczenia. Czy to nowy faworyt w *smart city*?

Lidar na pomoc inteligentnym miastom

Dotychczas lidar był stosowany głównie w zaawansowanych systemach wspomagania kierowcy (ADAS) w pojazdach. Okazuje się, że świetnie sprawdza się też jako narzędzie do wspomagania zarządzania ruchem miejskim, gdyż sprawnie wychwytuje zatory czy sytuacje zagrażające bezpieczeństwu na drogach. Wykorzystanie w czasie rzeczywistym trójwymiarowych danych dostarczanych przez lidar umożliwia miastom dogłębną analizę i na jej podstawie aktywne projektowanie bezpieczniejszych i bardziej efektywnych

systemów transportowych. W połączeniu ze sztuczną inteligencją pozwala rozpoznawać pieszych oraz innych uczestników ruchu drogowego z grupy podwyższonego ryzyka, np. rowerzystów, aby zapewnić im bezpieczeństwo, nie rozpoznając rysów twarzy.

Lidar – same zalety?

Tradycyjne urządzenia systemów dozoru wizyjnego, takie jak kamera czy radar, mają swoje ograniczenia – brak precyzji w zasięgu, słabe wykrywanie obiektów, niebezpieczne złudzenia optyczne. Uzyskanie szerokiego pola widzenia wymaga wielu urządzeń, a niekorzystne warunki oświetleniowe i pogodowe mogą osłabiać ich działanie.

Lidar zbiera dane przez cały rok, w każdych warunkach oświetleniowych i atmosferycznych, w czasie rzeczywistym. Jest multimodalny, wykrywa wszystkich użytkowników dróg, w tym pojazdy i pieszych. Ponadto jest efektywny kosztowo i łatwy w instalacji. Pojedynczy czujnik na słupie drogowym można wykorzystać w większości instalacji bez konieczności prowadzenia podziemnego okablowania. Zapewnia zaawansowaną analizę sytuacji w zakresie

bezpieczeństwa: przewidywanie, diagnozowanie i proaktywne rozwiązywanie kwestii bezpieczeństwa w ruchu drogowym.

Wyzwaniem dla wdrożenia lidar w inteligentnych miastach może być skalowanie projektu *smart city* od etapu pilotażowego do pełnego wdrożenia. Obawy budzą też koszty wdrożenia. Jednak biorąc pod uwagę to, że zazwyczaj potrzebny jest tylko jeden czujnik lidarowy na skrzyżowanie, a instalacja nie wymaga zmian w infrastrukturze, takich jak podziemne okablowanie, ogólny koszt systemów ruchu drogowego opartych na lidarze może być znacznie niższy niż systemów opartych na kamerach lub pętlach indukcyjnych.

Czy sam lidar wystarczy?

Lidar może stanowić uzupełnienie innych systemów zabezpieczeń. Przykładem może być miasto Rüsselsheim w Niemczech, które wdrożyło rozwiązanie BlueCity firmy Velodyne Lidar. Jest to rozwiązanie typu *full stack* do cyfrowego monitorowania i raportowania ruchu ciężarówek, które mają zakaz poruszania się po ulicach miasta.

Rozwiązania takie jak BlueCity dostarczają dane i narzędzia potrzebne do fuzji z innymi danymi, w tym z kamer sieciowych IP. To podejście zastosowano w Rüsselsheim, nakładając dane BlueCity na dane z kamer, odciążając policję w egzekwowaniu przepisów. ●



głos branży

Polskie miasta zmagają się dziś z wieloma problemami. Wysoka inflacja i konsekwencje wojny w Ukrainie nadal spędzają sen z powiek samorządowcom. Przedstawiciele różnych sektorów gospodarki podpowiadają, jak skutecznie zapewnić bezpieczeństwo i poprawiać komfort życia mieszkańcom.



Robert Bednarski

DYREKTOR DS. SMART CITY,
URZĄD MIEJSKI WROCŁAWIA

Wyzwania dotyczące realizacji idei smart city

Miasta, które chcą zaoferować swoim mieszkańcom wysoki komfort życia oraz wdrażają rozwiązania *smart*, muszą sprostać wielu wyzwaniom. Przekonaliśmy się o tym m.in. w związku z wybuchem pandemii czy wojną w Ukrainie, które doprowadziły do znacznego przyspieszenia cyfrowej transformacji miast. Rzeczywistość, w której obecnie żyjemy i funkcjonujemy, zachęca nas do coraz szerszego wykorzystania nowych technologii ułatwiających funkcjonowanie w świecie wirtualnym oraz realnym w miastach, a co za tym idzie, do coraz większego gromadzenia i przetwarzania dużych ilości różnego rodzaju danych. W związku z tym niezwykle ważnym wyzwaniem dla miast staje się zapewnienie cyberbezpieczeństwa.

Aby sprostać temu wyzwaniu, na początku czerwca 2022 r. Politechnika Wrocławska w partnerstwie z Miastem Wrocław, samorządem województwa dolnośląskiego oraz Zachodnią Izbą Gospodarczą

zainicjowała utworzenie makroklastra Technologie w Bezpieczeństwie Publicznym. Najważniejszym celem tego nowego przedsięwzięcia jest znalezienie nowych metod i rozwiązań technologicznych eliminujących cyberzagrożenia w przestrzeni publicznej.

Bezpieczeństwo i wysoka jakość życia mieszkańców to priorytety dla władz Wrocławia. Aby realizować je we właściwy sposób, należy przede wszystkim słuchać mieszkańców i skupiać się na ich potrzebach. Dlatego też w mieście jest realizowanych wiele projektów społecznych, również tych, które wykorzystują rozwiązania innowacyjne.

Biorąc pod uwagę powyższe, na początku bieżącego roku miasto przystąpiło do realizacji trzyletniego programu skierowanego do najstarszych mieszkańców „Teleopieka dla mieszkańców Wrocławia”. Głównym celem tego programu jest zwiększenie poczucia bezpieczeństwa seniorów w miejscu zamieszkania przy wykorzystaniu nowoczesnych technologii. W ramach programu 500 seniorów bezpłatnie otrzyma opaskę z przyciskiem życia oraz centralkę z przyciskiem wsparcia – urządzenia, za pomocą których będą mogli komunikować się z Centrum Teleopieki w celu wezwania pomocy, uzyskania wsparcia psychologicznego, uruchomienia sieci pomocowej. Świadczenie usługi rozpoczynamy już 9 maja.

Program „Teleopieka dla mieszkańców Wrocławia” jest odpowiedzią na projekt pilotażowy realizowany na początku pandemii w ramach CityLab Wrocław. Pilotaż pokazał nam, jak bardzo potrzebne są tego typu inicjatywy, zwłaszcza w sytuacji odizolowania czy wyłączenia społecznego, gdyż podnoszą one poczucie bezpieczeństwa najbardziej potrzebujących, a także prowadzą do ich aktywizacji społecznej i lepszego radzenia sobie w codziennym życiu.



Bartosz Dominiak

ZASTĘPCA BURMISTRZA DZIELNICY
URSYNÓW M.ST. WARSZAWY

Smart city to miasto odporne

Obyś żył w ciekawych czasach – tego życzenia (lub przekleństwa) samorządowcom mijającej za rok kadencji oraz tej kolejnej nie trzeba składać. Pandemia, wojna w Ukrainie, wymykająca się spod kontroli inflacja, niekorzystane dla samorządów zmiany podatkowe. Skutki tych zdarzeń w istotny sposób wpływają i będą wpływać na funkcjonowanie miast, a tym samym wdrażanie miejskiej inteligencji.

Pandemia i wojna zmieniły sposób myślenia o priorytetach miast. Do kluczowych wcześniej zmian klimatycznych doszły – jeszcze nie do końca zdefiniowane w wielu miastach – wyzwania związane z rozumianym wielowymiarowo bezpieczeństwem. Dotychczas bezpieczeństwo (z pewnymi wyjątkami, np. bezpieczeństwo na drogach) znajdowało się poza głównym nurtem miejskich debat. Dziś już tak nie jest, a *smart city* czasami zastępuje się pojęciem *resilient city* (miasto odporne).

Ta zmiana niesie ciekawą konsekwencję. Zmiany klimatyczne przez wielu były i są lekceważone, a tym samym nie wszystkie

działania samorządów w tym zakresie cieszyły się poparciem społecznym. Z kolei fizyczne zagrożenie bezpieczeństwa z zewnątrz zdecydowanie bardziej wpływa na wyobraźnię mieszkańców, więc i społeczne przyzwolenie na działania miast w tym zakresie wydaje się większe. W niektórych obszarach, choćby w przypadku bezpieczeństwa energetycznego (energooszczędność, przechodzenie na odnawialne źródła energii), występuje efekt synergii między walką ze skutkami zmian klimatycznych a walką o bezpieczne miasta. Mądre (*smart*) połączenie obu zagadnień może dać interesujące rezultaty.

Z kolei inflacja i zmiany podatkowe, których skutkiem są problemy finansowe samorządów, stawiają włodarzy miast przed trudnym definiowaniem priorytetów. Na wszystko nie wystarczy środków. Wydawać więcej środków na bezpieczeństwo czy jednak na podnoszenie – być może czasami nadmierne – jakości życia w mieście? A warto przy tym pamiętać, że wydatki na bezpieczeństwo mają dwie cechy: są w zasadzie nieograniczone, a w sytuacji, gdy nic złego się nie dzieje – są dla mieszkańców de facto niewidoczne, co wielu może odczytywać jako zbędne.

To są dzisiejsze dylematy, przed którymi stoją włodarze miast. Od ich wyborów będzie zależało i bezpieczeństwo, i rozwój powierzonych im miejskich organizmów.



Rafał Batkowski

RBS

Zwiększenie poczucia bezpieczeństwa mieszkańców

Przyjmijmy na wstępie trzy założenia: miasta różnią się od siebie poziomem bezpieczeństwa; ten stan jest zmienny w czasie, poczucie bezpieczeństwa nie jest tożsame z realnym stanem zagrożeń. Warto szczególnie interesować się bezpieczeństwem obszarów zurbanizowanych, kluczowych z punktu widzenia potencjalnych zagrożeń dla wielkich skupisk ludzkich, infrastruktury (w tym krytycznej), siedzib władz, centrów bankowych, inwestycyjnych, analitycznych i największych podmiotów gospodarczych.

Analizując stan zagrożeń w Polsce, zauważa się wzrost przestępczości ogółem w 2022 r. o prawie 5% w stosunku do roku poprzedniego (przestępstwa stwierdzone). Zanotowano 882 278 zdarzeń, w tym m.in. 509 281 przestępstw kryminalnych, co stanowi wzrost o 1,7%, oraz 264 857 przestępstw gospodarczych – wzrost o 17,5%. Spośród zdarzeń kryminalnych najwięcej było kradzieży: 124 057, co daje wzrost o ponad 11%. Należy jednak dostrzec także spadki zagrożenia w odniesieniu do: zabójstw (507) – mniej o 20%; zgwałceń (1117) – spadek o 0,9% oraz przestępstw rozbójniczych (4832) – mniej o 0,9%, w badanym okresie, co jest dobrym prognozykiem, mając na uwadze spadek o ponad 50% przestępczości w Polsce w ciągu ostatnich 20 lat.



Należy jednak pamiętać o cyberzagrożeniach, które lawinowo rosną i dotyczą wielu z nas. Jednocześnie warto spojrzeć na wskaźnik zagrożenia przestępczością na 100 tys. mieszkańców w kilku największych i najbardziej zagrożonych miastach (dane KGP): Katowice – 6749; Wrocław – 3803; Gdańsk – 3333; Warszawa – 3173; Poznań – 3017; Kraków 2872. Duże aglomeracje wymagają strategii zapobiegawczych i skutecznych systemów reagowania.

Niezależnie od powyższego, powinniśmy interesować się poczuciem bezpieczeństwa mieszkańców, na które wpływa wiele czynników oraz subiektywne postrzeganie środowiska bezpieczeństwa, nie tylko w lokalnym wymiarze. Dzisiaj, poza przestępczością, to również sytuacja na Ukrainie, ale także wysoka inflacja, ceny energii, gazu bezpośrednio wpływają na naszą sytuację osobistą, a nierzadko implikują wybory dotyczące sposobów organizacji życia codziennego, w tym wydatkowania środków na bezpieczeństwo. Z takimi wyzwaniami mierzą się również miasta, które często nie znajdują odpowiednich źródeł finansowania inwestycji służących bezpieczeństwu ludzi.

Co można zrobić w tej sytuacji? Wydaje się, że tylko świadome, zrównoważone rozwojowo, poprzedzone analizami decyzje strategiczne, w perspektywach długo- i krótkoterminowych mogą przynieść oczekiwane efekty. Budowanie miejskich strategii, uwzględniających sprawy bezpieczeństwa (dzisiaj to rzadkość) oraz ich wdrożenie i nowoczesne zarządzanie oparte na rzetelnych danych powinno uwzględniać:

- transformację cyfrową, która zawsze powinna rozwijać komponent SAFE CITY, poza SMART CITY, w szczególności wieloźródłową analizę danych w celu wsparcia zarządzających w procesie decyzyjnym, inteligentne systemy zarządzania infrastrukturą, transportem oraz wykorzystanie najnowocześniejszych technologii bezpieczeństwa dla dobra obywateli;
- wystandaryzowane badanie miast w celu rzetelnej, trafnej odpowiedzi na wyzwania i oczekiwania mieszkańców, z uwzględnieniem predykcji niebezpiecznych procesów;
- przeznaczenie większych zasobów na rozwój technologii chroniących urzędy (i spółki miejskie, szpitale, placówki edukacyjne itp.) przed cyberzagrożeniami – budować odporność infrastruktury oraz świadomość mieszkańców w tym zakresie, dostarczyć rzeczywiste, bezpłatne wsparcie w postaci aplikacji, poradnictwa;
- strategię zapobiegawczą dotyczące zachowań przemocowych oraz ekstremistycznych, radykalnych powinny zmierzać w kierunku polityk włączania społecznego, a nie wykluczania, stanowczo reagować w przypadku identyfikacji zagrożenia;
- potencjał prywatnego sektora bezpieczeństwa;
- analizę ryzyk i podatności miejsc publicznych na zagrożenia, czyli stosowanie zaawansowanych technologicznie systemów zabezpieczających oraz poszukiwanie wielopodmiotowego współdziałania interesariuszy (m.in. policji, służb ratowniczych, lokalnych władz, organizacji i mieszkańców);
- społeczną partycypację w kreowaniu bezpieczeństwa, w tym konsultacje społeczne oraz budżety obywatelskie dedykowane pomyśłom mieszkańcom;
- policję angażującą się w działania prospołeczne i proaktywne, blisko współpracującą z samorządem, posiadającą zdolności do natychmiastowego interweniowania w obliczu zagrożenia;
- wykorzystanie środków unijnych na rozwijanie strategii, technologii i praktyk służących bezpieczeństwu społeczności lokalnych.



Bogumił Szymanek

AXIS COMMUNICATIONS

Udział mieszkańców w rozwiązywaniu problemów lokalnych

Prawdziwe *smart city* to miejsce, gdzie zaawansowane zintegrowane technologie są stosowane po to, aby mieszkańcom żyło się lepiej. Wiele rozwiązań postrzega się z perspektywy całego miasta. I słusznie, ponieważ kluczowe są np. przepustowość miejskich dróg i komunikacja, dostęp do usług miejskich, jakość powietrza. Ale w takim podejściu, znanym jako *smart city* 2.0 brakuje udziału społeczności lokalnych w rozwoju inteligentnego miasta i zaspokajaniu lokalnych potrzeb.

Obecnie miasta otwierają się na aktywny udział mieszkańców w rozwiązywaniu miejscowych problemów, które mają bezpośredni wpływ i są odczuwalne przez konkretne społeczności. Wchodzimy więc w *smart city* 3.0 określane niekiedy nazwą Human Smart Cities. Dzięki dostępowi do projektów obywatelskich mieszkańcy wskazują obszary w ich najbliższym otoczeniu, które wymagają zmiany, by np. wzmocnić poczucie bezpieczeństwa, wpływając bezpośrednio na codzienne życie rodzin i współmieszkańców.

W tego typu inicjatywach pomagają działania, takie jak kampania AXIS „Bezpieczny zaułek”, gdzie miasta, wskazując potrzebę, mogą uzyskać realne wsparcie projektowe i technologiczne w poprawie bezpieczeństwa w najbliższym otoczeniu mieszkańców.

Przykładem będzie instalacja kamery z radarem w pobliżu szkoły, dzięki czemu lepiej kontrolowana jest prędkość samochodów i zwiększone bezpieczeństwo uczniów. Kamera oraz głośnik sieciowy mogą zredukować liczbę niepożądanych zachowań i aktów wandalizmu na boisku szkolnym albo ograniczyć dzikie wysypiska śmieci. Wiele takich małych inicjatyw poprawia życie mieszkańców całego miasta i realizuje cele prawdziwego *smart city*.



Marcin Walczuk

BCS

Miasta przyszłości już dziś

Nowoczesne miasto jest coraz bardziej zdigitalizowane, kierunek jego rozwoju wyznacza idea *smart city*. Inteligentne aglomeracje będą działać efektywniej, optymalizując jakość usług dla mieszkańców oraz przedsiębiorstw. Obecnie żyjemy w społeczeństwie informacyjnym, czerpiemy i przetwarzamy olbrzymie ilości danych, aktywnie korzystając z różnego rodzaju usług. Dzięki zastosowaniu rozwiązań informatyczno-komunikacyjnych efektywniej wykorzystujemy zasoby miasta, które poprawiają jakość naszego życia. Dziś,

aby kupić bilet w autobusie czy metrze, nie trzeba już szukać kiosku czy biletomatu, wystarczy skorzystać z aplikacji, a skasowanie biletu dokonuje się przez zeskanowanie kodu QR w danym środku transportu. Aby wymiana informacji była jednak możliwa, potrzebne są właściwe rozwiązania infrastrukturalne.

Rozwój nowoczesnych technologii telekomunikacyjnych, w tym łączy światłowodowych czy sieci komórkowej 5G, jest w tym przypadku niezbędny dla sprawnego funkcjonowania miasta przyszłości. Ilość danych, które tworzymy i odbieramy, będzie rosła, dlatego tak ważne są prędkość i przepustowość sieci, do których mamy dostęp. Każdy użytkownik smartfona korzystający z połączenia z Internetem, przeglądający strony www, media społecznościowe czy uruchamiający zdalnie odkurzacz w swoim domu generuje ruch sieciowy. Do tego dochodzi coraz większa liczba urządzeń IoT i różnego rodzaju czujników, np. wspomagających systemy monitorowania miejsc parkingowych, zautomatyzowane systemy zarządzania ruchem ulicznym czy system monitoringu miejskiego.

Poprawa i zapewnienie odpowiedniego poziomu bezpieczeństwa mieszkańców jest jednym z głównych założeń rozwijającego się miasta. Stale rosnąca liczba kamer w systemie monitoringu miejskiego pozwala na dokładniejszą analizę potencjalnych zagrożeń, może również przyspieszyć reakcję odpowiednich służb na niebezpieczne sytuacje. Dzięki coraz szerszemu wykorzystaniu sztucznej inteligencji w urządzeniach systemów monitoringu wizyjnego algorytmy są w stanie rozpoznać zachowanie noszące znamiona przestępstwa. Informacje o zdarzeniach mogą być generowane bez udziału operatorów systemu. Oczywiście nie chodzi o całkowite wyeliminowanie człowieka, ale umożliwienie mu skupienia się na zdarzeniach, których system nie jest w stanie w jednoznaczny sposób sklasyfikować.

W ostatnich latach również jakość obrazu przekazywanego przez kamery diametralnie się poprawiła. Teraz rozdzielczość jest już na tyle wysoka, że nawet z dużej odległości można zidentyfikować numer tablicy rejestracyjnej czy rozpoznać twarz człowieka. Na podstawie dodatkowych informacji, które „dostajemy” z systemu monitoringu,

można później w łatwy i zdecydowanie szybszy sposób wyszukać potrzebne nagrania, co przekłada się na skuteczniejsze działanie systemu bezpieczeństwa miasta i mieszkańców. Tu mogą pojawiać się obawy o zachowanie prywatności mieszkańców – jest jednak cienka granica między zapewnieniem wygody i bezpieczeństwa a inwigilacją obywateli.



Michał Swoboda

HIKVISION POLSKA

Koncepcja bezpiecznego miasta

W ostatnich latach coraz większy nacisk kładzie się na podniesienie poziomu bezpieczeństwa miast, a tym samym poprawienie komfortu życia ich mieszkańców. Koncepcja „bezpiecznego miasta” wykracza poza tradycyjne zapobieganie przestępczości i obejmuje inne aspekty bezpieczeństwa, takie jak zagrożenia środowiskowe, klęski żywiołowe i zagrożenia zdrowia publicznego. *Safe City* 2.0 to kolejna ewolucja tego procesu wykorzystująca technologię do tworzenia bezpieczniejszych i bardziej odpornych miast.

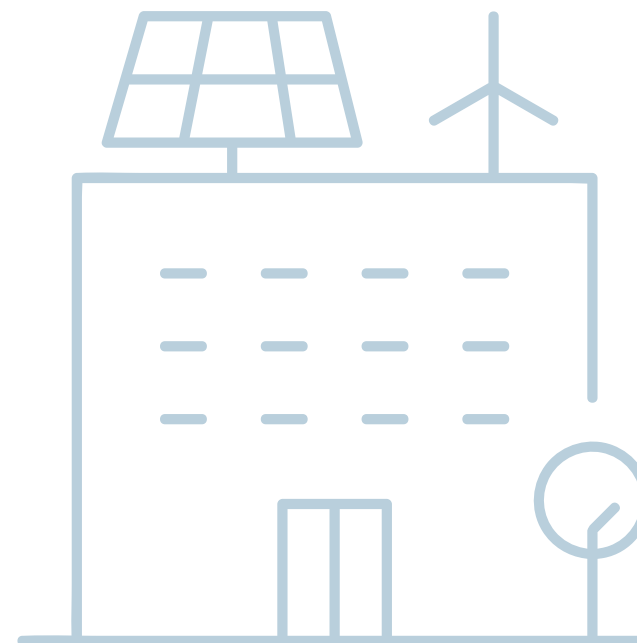
Jedną z kluczowych cech *Safe City* 2.0 jest wykorzystanie zaawansowanej analityki i uczenia maszynowego do przewidywania przestępczości i zapobiegania im. Analizując dane z różnych źródeł, takich jak kamery monitoringu wizyjnego, media społecznościowe i raporty o przestępczości, miasta mogą identyfikować wzorce i przewidywać potencjalne punkty zapalne. Informacje te mogą być wykorzystane do bardziej efektywnego rozmieszczenia zasobów policyjnych i zapobiegania przestępczości.

Innym ważnym aspektem jest wykorzystanie inteligentnych czujników i urządzeń IoT (Internet rzeczy) do monitorowania i wykrywania potencjalnych zagrożeń. Na przykład czujniki mogą wykrywać wycieki gazu, pożary i inne zagrożenia środowiskowe, natomiast urządzenia IoT – monitorować jakość powietrza, temperaturę i poziom wilgotności. Dzięki wczesnemu wykrywaniu tych zagrożeń miasta mogą podejmować proaktywne działania w celu zapobiegania katastrofom i ochrony swoich mieszkańców.

Inną ważną inicjatywą jest włączenie społeczności lokalnej do budowania bezpieczeństwa w ich miejscu zamieszkania. Obejmuje to takie inicjatywy, jak programy obserwacji sąsiedzkiej, patrole obywatelskie i policję środowiskową. Angażując mieszkańców w proces bezpieczeństwa, miasta mogą budować zaufanie i wzmacniać poczucie własności i odpowiedzialności za dobrobyt swoich społeczności.

Miasta nie są w stanie same stworzyć bezpiecznego środowiska dla mieszkańców, do osiągnięcia sukcesu niezbędne jest partnerstwo z sektorem prywatnym, środowiskiem akademickim i społeczeństwem obywatelskim. Pracując razem, miasta mogą wykorzystać swoje mocne strony i zasoby, aby stworzyć bardziej innowacyjne i skuteczne rozwiązania.

Safe City 2.0 stanowi więc kolejną ewolucję w dziedzinie bezpieczeństwa miejskiego. Wykorzystując technologię, dane i zaangażowanie społeczności, miasta mogą stworzyć mieszkańcom bezpieczniejsze,



bardziej odporne i łatwiejsze do życia środowisko. Choć wyzwania są znaczące, korzyści płynące z koncepcji bezpiecznego miasta 2.0 są oczywiste, a potencjał transformacji jest ogromny.



Anna Twardowska
NEDAP SECURITY MANAGEMENT

Wyzwania w modelu pracy hybrydowej

Smart building obejmuje rozwiązania i systemy mające na celu zaspokojenie różnych potrzeb użytkowników, także w zakresie zwiększenia funkcjonalności i bezpieczeństwa obiektów. Rozwiązania z tego zakresu mają zapewnić większy komfort pracy, niższe zużycie energii i uprościć zarządzanie obiektem.

Takim rozwiązaniem są także lockery – szafki do przechowywania. W ostatnich latach nastąpiło wiele zmian w formie naszej pracy. W dużej części organizacji na stałe zagościła już praca hybrydowa, która wprowadziła zmiany w naszym otoczeniu, a także wygenerowała wiele wyzwań. Zmieniły się nasze zwyczaje i codzienne praktyki. Zamiast na stałe przypisanych do poszczególnych pracowników biurek mamy *hot desks*. Pojawiła się także idea czystego biurka gotowego do pracy dla innej osoby, a jednocześnie potrzeba zabezpieczenia dokumentów i rzeczy osobistych pracowników. To wygenerowało potrzebę przechowywania tych rzeczy, często w rozproszonych miejscach w biurze. Dodatkowe ważne aspekty to zachowanie prywatności i łatwiejsze utrzymanie porządku w przestrzeniach biurowych. Dlatego też lockery – szafki do przechowywania – stają się niezbędnym elementem biura i ważną inwestycją mającą na celu zapewnienie bezpiecznego i wygodnego miejsca pracy.

Aby odpowiednio zabezpieczyć takie szafki, warto zainwestować w rozwiązania, które zapewniają dostęp do nich poprzez użycie karty dostępu, tej samej, z którą pracownik porusza się po biurze. Można także skorzystać z kart wirtualnych i smartfonów, które są coraz częściej stosowane w inteligentnych budynkach. Aby jeszcze bardziej poprawić wygodę korzystania z szafek pracowniczych, w niektórych biurach zdecydowano się na wykorzystanie systemów rozpoznawania twarzy. Porównują one twarz użytkownika ze wzorcem biometrycznym, który jest już używany przez system kontroli dostępu.

W elastycznym zarządzaniu szafkami duże znaczenie ma także wykorzystanie jednej platformy do zarządzania lockerami i kontrolą dostępu. Daje to dużą przewagę w procesie nadawania uprawnień do szafek. Dodatkowym plusem jednej platformy do zarządzania lockerami i SKD jest wykorzystanie w szafkach zaimplementowanych integracji w systemach kontroli dostępu.

Dobrym przykładem jest integracja z systemami HR. Pracownik, który zostaje zatrudniony np. w dziale marketingu, może mieć automatycznie nadany dostęp do wspólnej szafki na korespondencję działową. W momencie zakończenia pracy w danej organizacji i odnotowania tego faktu w systemie HR automatycznie straci uprawnienia do przypisanych szafek.

Lockery są świetnym rozwiązaniem także w miejscach publicznych, umożliwiają gościom przechowywanie rzeczy osobistych. W przypadku tej grupy użytkowników warto zastosować kody QR – to bardzo efektywna i funkcjonalna forma udzielania dostępu w wyznaczonym miejscu na jednorazowe użycie. Dodatkowe integracje pozwalają na wykorzystanie szafek w roli biurowych paczkomatów czy dla lepszej dystrybucji sprzętu przez dział IT dla nowych pracowników bądź oddawanie do naprawy zepsutych laptopów i dystrybucję naprawionych urządzeń. Zastosowań lockerów jest wiele, a ich coraz powszechniejsze wykorzystanie w biurach z pewnością zwiększy pomysłowość i wykreuje nowe obszary zastosowań.



Daniel Kamiński
SMART-I

Kontrola dostępu przystosowana do hybrydowego modelu pracy

Jesteśmy uczestnikami cyfrowej transformacji, w której ramach wiele organizacji stara się dostosować do nowoczesnych hybrydowych sposobów pracy. Proces ten trwa od dłuższego czasu, a w trakcie pandemii przyspieszył. Firmy szybko inwestowały w technologie, aby umożliwić pracownikom pracę i łączenie się z firmowymi systemami. Niestety w trakcie pandemii wdrażano wiele odmiennych technologii, które były niekompatybilne z cyfrowymi ekosystemami budynków biurowych.

W trakcie wdrażania cyfrowej transformacji często pomijany był aspekt kontroli dostępu do fizycznych budynków i przestrzeni. Brakowało planowania integracji systemów bezpieczeństwa z narzędziami wykorzystywanymi w miejscu pracy. Hybrydowe modele pracy spowodowały nieprzewidywalny napływ osób do budynków biurowych, co oznacza, że zarządzanie miejscami pracy, stanowiskami parkingowymi oraz obsługą klientów i gości stało się trudniejsze niż kiedykolwiek.

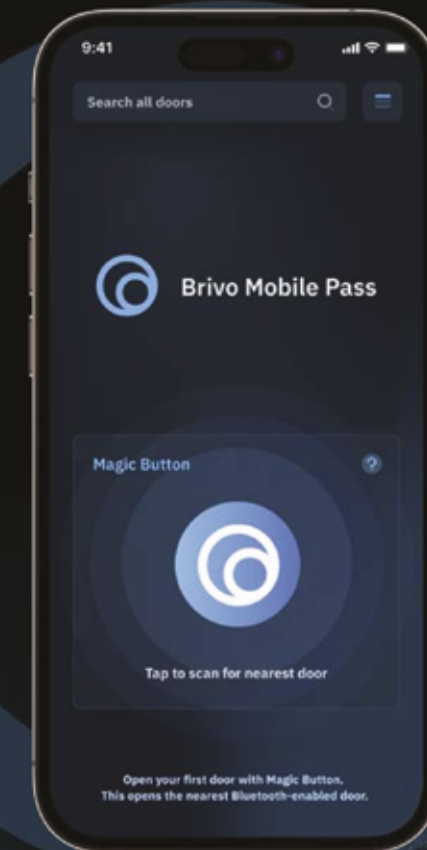
Z tego względu firmy potrzebują kompleksowych scentralizowanych systemów bezpieczeństwa, które są przystosowane do pracy hybrydowej i mogą płynnie integrować się z innym oprogramowaniem. Korzystanie ze zintegrowanych platform ułatwia podejmowanie decyzji na podstawie gromadzonych danych. Informacje o zajętości budynku, wykorzystaniu przestrzeni oraz o tym, kiedy pracownicy wchodzić do określonych obszarów, można zintegrować z innymi danymi zarządczymi, takimi jak zużycie mediów, w celu zmniejszenia ogólnego zużycia energii oraz obniżenia zbędnych kosztów operacyjnych.

Niezależnie od tego, czy ludzie pracują zdalnie, czy w biurze, wszystkie systemy muszą być bezpieczne. W modelu pracy hybrydowej trudniej jest kontrolować to, z jakich narzędzi korzystają pracownicy. W firmach z rozproszoną infrastrukturą trudniej jest też integrować tradycyjne systemy bezpieczeństwa z systemami biznesowymi. Jedynym przyszłościowym sposobem jest korzystanie z rozwiązań opartych na chmurze. ●




DOSTĘP JEST PRZYSZŁOŚCIĄ INTELIGENTNYCH BIUR

ZOPTYMALIZUJ SWOJE NIERUCHOMOŚCI DZIĘKI KONTROLI DOSTĘPU BRIVO



Technologia zabezpieczeń klasy korporacyjnej dla każdego rodzaju obiektu

60+
KRAJÓW NA
CAŁYM ŚWIECIE



Kontrola dostępu i dane wideo, dzięki którym Twoje budynki staną się bardziej inteligentne

90+
TYSIĄCE
WDROŻEŃ



Możliwości integracji, aby połączyć istniejące inwestycje technologiczne

450Mkw
NIERUCHOMOŚCI W
ZARZĄDZANIU



866.692.7486 | brivo.com

Brivo oferuje kompleksowy zestaw narzędzi dostosowanych do Twoich potrzeb w zakresie kontroli dostępu. Dowiedz się więcej na www.brivo.com/solutions/commercial-real-estate/

Przedstawiamy mapę dużych inwestycji, które są w trakcie realizacji lub dopiero się rozpoczną. Termin ich ukończenia nie upływa przed IV kwartałem 2023 r. W poprzednim numerze przedstawiliśmy obszerną listę, na której znalazło się ponad 20 ogólnopolskich dużych inwestycji z różnymi terminami realizacji. Niektóre z nich upływają niebawem, ale wiele jest odległych. W tym numerze uzupełniamy mapę o kolejne projekty – takie, na których realizację podpisano umowy w ciągu ostatnich dwóch miesięcy. Zachęcamy do śledzenia kolejnych wydań „a&s Polska”, by poznać pełną listę najważniejszych aktualnych inwestycji w Polsce.

Adela Prochyra, a&s Polska

Mapa inwestycji

BUDIMEX

Co: **EKOLOGICZNA MYJNIA POCIĄGÓW PKP**

Gdzie: Kraków, ul. Składowa 17, tor 11

Kiedy: I kwartał 2024 r.

1

INSTAL KRAKÓW

Co: **WYMIANA URZĄDZEŃ ODWADNIAJĄCYCH WRAZ Z RUROCIĄGAMI TECHNOLOGICZNYMI W OCZYSZCZALNI ŚCIEKÓW PODLESIE**

Gdzie: Katowice

Kiedy: 15.11.2023 r.

2

Co: **MODERNIZACJA UKŁADÓW POMPOWYCH NA STACJI UZDATNIANIA WODY BIBIELA**

Gdzie: Katowice

Kiedy: 4.05.2024 r.

3

Co: **MODERNIZACJA GOSPODARKI ELEKTROENERGETYCZNEJ, CIEPLNEJ I BIOGAZOWEJ NA TERENIE OCZYSZCZALNI ŚCIEKÓW PŁASZÓW PRZY UL. KOŚCIARZY 3**

Gdzie: Kraków

Kiedy: 17.01.2024 r.

4

STRABAG

Co: **WIECHA NA BUDYNKU NOWEGO BŁOKU SZPITALA WOJEWÓDZKIEGO W LUBLINIE**

Gdzie: Lublin

Kiedy: IV kwartał 2023 r.

5

TRAKCJA S.A.

Co: **ZAPROJEKTOWANIE I WYKONANIE REMONTU ROZDZIELNIC PRĄDU STAŁEGO NA STACJI METRA KABATY**

Gdzie: Warszawa

Kiedy: 6.10.2023 r.

6

UNIBEP

Co: **BUDOWA KAMPUSU AKADEMII MUZYCZNEJ IM. FELIKSA NOWOWIEJSKIEGO**

Gdzie: Bydgoszcz

Kiedy: 06.09.2023

7

WARBUD + TKT ENGINEERING

Co: **II ETAP BUDOWY CENTRALNEGO ZINTEGROWANEGO SZPITALA KLINICZNEGO W POZNANIU**

Gdzie: Poznań, Grunwald

Kiedy: kwiecień 2023-październik 2025

8

Co: **PRZEBUDOWA UNIWERSYTECKIEGO SZPITALA DZIECIĘCEGO W LUBLINIE**

Gdzie: Lublin

Kiedy: IV kwartał 2023

9

Co: **MODERNIZACJA AQUAPARKU**

Gdzie: Polkowice

Kiedy: czerwiec 2024

10





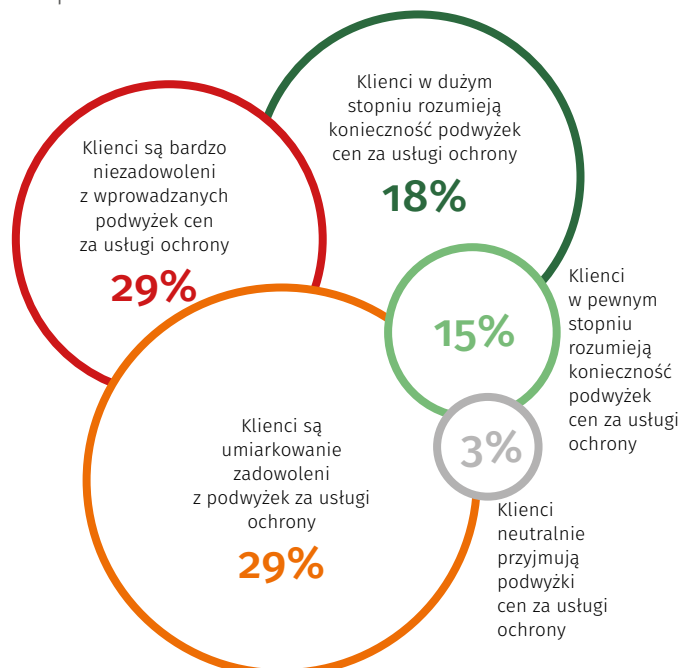
Branża bezpieczeństwa w Polsce. Raport Polskiego Związku Pracodawców Ochrona

Jak przedsiębiorstwa z branży oceniają rynek i jak radzą sobie z wyzwaniami? Na to pytanie odpowiada raport *Branża bezpieczeństwa w Polsce: szanse, zagrożenia, kierunki rozwoju* opracowany przez Polski Związek Pracodawców Ochrona.

Wypracowanie kompromisu cenowego to jedno z największych wyzwań ostatnich miesięcy dla firm z branży ochrony. Wynagrodzenie pracowników stanowi ok. 80% wszystkich kosztów usług tego sektora, ale sytuacja gospodarcza skłania wiele przedsiębiorstw będących klientami branży ochrony do ograniczania wydatków. Niestety, także tych na bezpieczeństwo.

Polska branża ochrony osób i mienia – rynek o wartości 11 mld zł – funkcjonuje w bardzo wymagającym, pod wieloma względami, otoczeniu. – W 2022 r. firmy ochrony zmagają się z problemami w związku z trudną sytuacją rynkową, wysoką inflacją, podwyżkami minimalnego wynagrodzenia za pracę czy rekordowo niską stopą bezrobocia skutkującą brakiem kandydatów do pracy – podkreśla Tomasz Wojak, prezes zarządu Polskiego Związku Pracodawców Ochrona. – Z kolei wydarzenia ostatnich kilku lat, takie jak pandemia COVID-19 czy wojna w Ukrainie, znacznie

Czy podwyżki cen za usługi ochrony, związane z zaplanowanymi na 2023 rok wysokimi podwyżkami stawek minimalnego wynagrodzenia za pracę, mają dostrzegalny wpływ na nastroje państwa klientów?



obniżyły poczucie bezpieczeństwa Polaków. W raporcie podsumowujemy opinie przedstawicieli branży, co – mam nadzieję – stanowi punkt wyjścia do debaty o usługach związanych z bezpieczeństwem.

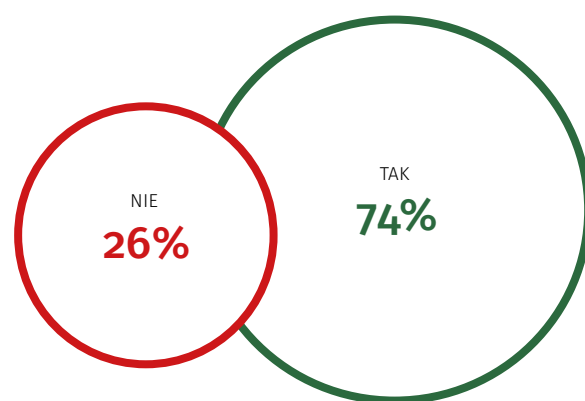
Dokument powstał na podstawie badania przeprowadzonego w 2022 r. wśród około 70 przedstawicieli firm zrzeszonych w Polskim Związku Pracodawców Ochrona oraz Polskiej Izbie Ochrony. W raporcie poza wynikami badań znalazły się komentarze ekspertów – przedstawicieli Business Centre Club, Federacji Przedsiębiorców Polskich, Polskiej Organizacji Handlu i Dystrybucji, Polskiej Rady Centrów Handlowych oraz Stowarzyszenia Branży Eventowej.

Sytuacja gospodarcza największym wyzwaniem

Miniony rok był dla branży ochrony podwójnie trudny. Firmy musiały działać w niełatwych warunkach gospodarczych, a równocześnie negocjować z klientami wyższe stawki za usługi. Przedstawiciele firm ochrony zapytani o wyzwania, z którymi musieli się mierzyć, w pierwszej kolejności wskazują na konieczność renegotjacji umów z klientami w związku z rosnącą presją na wzrost wynagrodzeń wśród pracowników (ponad 70% odpowiedzi). Niemal 2/3 respondentów (64%) wskazuje, że usługobiorcy byli niezadowoleni z tak wysokiego wzrostu cen. Główny powód? Dla ponad połowy ankietowanych (55%) było pogorszenie koniunktury gospodarczej w naszym kraju (m.in. wysoka inflacja) i związany z tym spadek zamówień. Niemal połowa (45%) uczestników badania wskazuje z kolei na konieczność sprostania obciążeniom wynikającym z nowych przepisów (np. Polskiego Ładu).

Jako powód najczęściej podają brak wykwalifikowanych pracowników (głównie osób z pozwoleniem na posiadanie broni, ponieważ w trakcie pandemii policja nie organizowała egzaminów dających takie uprawnienia) oraz niskie płace w branży. Łukasz Koch, wiceprezes Polskiego Związku Pracodawców Ochrona, podaje kolejne istotne czynniki: transparentność form zatrudnienia, zabezpieczenie odpowiednich warunków socjalnych

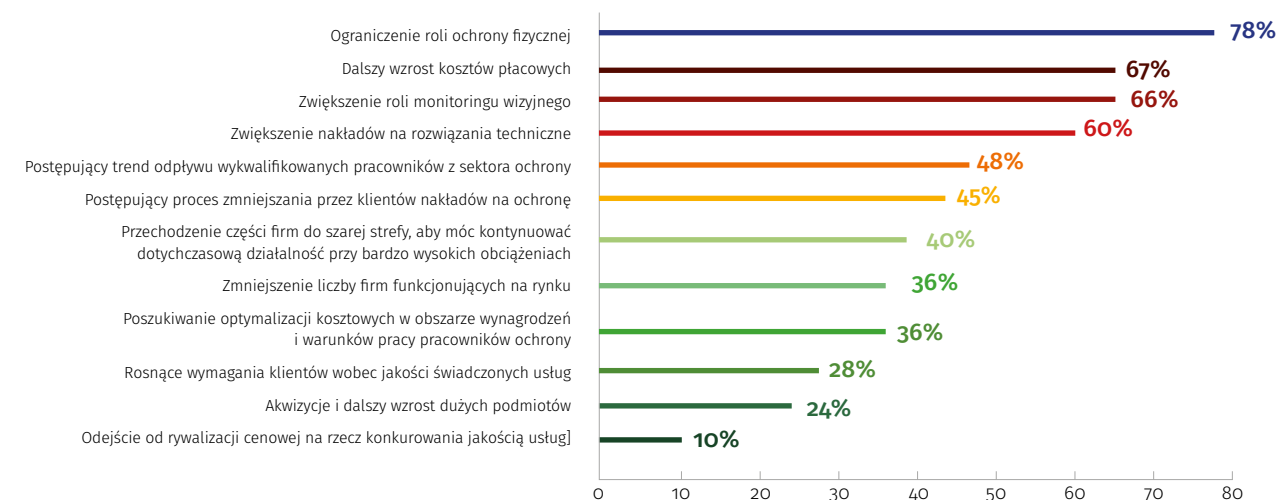
Czy w 2022 roku zwiększyli państwo nakłady na rozwiązania techniczne wspomagające lub zastępujące świadczone usługi ochrony fizycznej?



Co jest największym wyzwaniem dla państwa firmy w 2022 roku?



Co czeka państwa zdaniem branżę ochrony w perspektywie 5 najbliższych lat?



i standardów BHP, a także inwestowanie w rozwój pracowników. – Oferta pracodawców z sektora ochrony często nie jest atrakcyjna dla pracowników, którzy znajdują ciekawsze możliwości zatrudnienia w innych sektorach – mówi Łukasz Koch. – Potrzebna jest fundamentalna zmiana sposobów zatrudniania, wynagradzania, warunków pracy oraz kształtowania relacji pracowniczych w firmach z branży ochrony – nie jest to łatwe, ale konieczne, jeżeli oczekujemy poprawy sytuacji.

Rosnąca rola automatyzacji

W sektorze ochrony obserwujemy trend nieustannego rozwoju technologicznego. Niemal 74% respondentów badania deklaruje, że w 2022 roku zwiększyły nakłady na rozwiązania techniczne wspomagające lub zastępujące ochronę fizyczną.

Transformację technologiczną w firmach z sektora ochrony przyspieszyła pandemia. W związku z zapowiadanymi podwyżkami za usługi ochrony klienci stali się bardziej otwarci na rozwiązania technologiczne w ochronie – wskazuje tak 49% uczestników badania.

Respondenci nie mają wątpliwości, że ten trend będzie się utrzymywał. Odpowiadając na pytanie, co ich zdaniem czeka branżę ochrony w perspektywie 5 najbliższych lat, wskazują właśnie świadczenie usług z wykorzystaniem technologii (ograniczenie roli ochrony fizycznej – 78%, zwiększenie roli monitoringu wizyjnego – 66%, zwiększenie nakładów na rozwiązania techniczne – 60%). Jarosław Kot, członek zarządu Polskiego Związku Pracodawców Ochrona, wyjaśnia: – Kierunek ten wydaje się nieuchronny ze względu na rosnące koszty pracy stanowiące przeważającą

część wynagrodzenia za usługi ochrony. Alternatywa w postaci korzystania z nowoczesnych rozwiązań staje się więc sposobem na powstrzymanie wzrostu kosztów i daje możliwość zabezpieczenia chronionych obiektów we właściwy sposób.

Dla przedsiębiorców czas kryzysu, razem z towarzyszącą mu inflacją, wiąże się z koniecznością cięcia kosztów. Firmy oszczędzają m.in. na bezpieczeństwie, szczególnie w obliczu szybko rosnących kosztów usług z tego zakresu. Tomasz Wojak, prezes Polskiego Związku Pracodawców Ochrona, podkreśla: – Klienci akceptują wzrost wynagrodzeń pracowników ochrony w wyniku rządowych regulacji oraz niskiego bezrobocia, które skutkuje brakiem chętnych do pracy. Jednocześnie klienci naszego sektora ograniczają zakres usług wykonywanych przez ludzi, likwidują posterunki ochrony, zmniejszają liczbę godzin przeznaczonych na ochronę. To w konsekwencji może oznaczać, że przedsiębiorstwa narażają się na wyższe straty spowodowane niewystarczającą ochroną mienia. Efekty oszczędności widać jednak od razu, a straty – dopiero po jakimś czasie, np. po inwentaryzacji. Jako PZPO zachęcamy więc klientów branży ochrony, by podchodzili do kwestii ochrony długofalowo, traktując wydatki na te usługi jak inwestycję, która na pewno się zwróci.

Pełny raport *Branża bezpieczeństwa w Polsce: szanse, zagrożenia, kierunki rozwoju* jest dostępny na stronie PZPO. ●



Polski Związek Pracodawców Ochrona
ul. Koszykowa 61, 00-667 Warszawa
biuro@pzpochrona.pl
www.pzpochrona.pl



Lawinowy wzrost liczby kradzieży

Ostre hamowanie polskiej gospodarki i rekordowo wysoka inflacja, a co za tym idzie biedniejące społeczeństwo – tak rodzi się palący problem kradzieży.
Tomasz Grzelak

Statystyki policyjne pokazują wprost, że włamania i kradzieże stają się dziś ogromnym wyzwaniem. Według danych Komendy Głównej Policji w ubiegłym roku stwierdzono 32,8 tys. kradzieży w sklepach, to o 31,1% więcej niż w 2021 r., kiedy takich przypadków odnotowano ok. 25 tys. Liczba wykroczeń, czyli kradzieży towarów o wartości nieprzekraczającej 500 zł, podczas 12 miesięcy zeszłego roku wyniosła ponad 234,3 tys. W 2021 r. takich zdarzeń odnotowano 192,8 tys., co

oznacza wzrost o 21,5%. Dane te pokazują wyraźnie, z jaką skalą mamy do czynienia.

Problem najbardziej dotyka branżę spożywczą

Kradzieże w sklepach dokonywane są na różne sposoby. Od tych najprostszych, jak pochwycenie towaru umieszczonego najbliżej drzwi wejściowych i wybiegnięcie z nim, przez chowanie artykułów do toreb lub kieszeni (często specjalnie w tym celu przygotowanych), po oszukiwanie przy kasie samoobsługowej, czyli albo pomijanie wybranych produktów, albo celowe zamienianie kodów kreskowych i skanowanie tańszych rzeczy zamiast faktycznie droższych. Jednorazowo podczas większych zakupów oszust może wynieść towar za 100-150 zł. Borykające się z niedoborem pracowników sklepy chętnie montują tego rodzaju kasy. Jedna z dużych sieci handlowych w części swoich sklepów w Niemczech z powodu wysokich strat związanych z oszustwami przy kasach samoobsługowych zdecydowała się je zdemontować.

Włamania

Statystyki są coraz bardziej niepokojące. Rośnie liczba kradzieży sklepowych, wzrasta liczba włamań do domów i mieszkań. Jak podaje portal rp.pl, tylko na Mazowszu do końca listopada 2022 r. policja odnotowała 874 włamania do mieszkań. To o ponad 40% więcej niż rok wcześniej i aż o 75% więcej niż w roku 2020. W ciągu ostatnich dwóch lat w niektórych miastach (np. w Radomiu) liczba włamań zwiększyła się dwukrotnie. Te dane nie uwzględniają Warszawy i okolic, gdzie wprowadził wzrost był mniejszy (o 6,5%), ale liczba włamań wzrosła. Komenda Stołeczna Policji zarejestrowała w tym okresie 4524 takie przypadki.

Aby dostać się do obiektu, przestępcy stosują różne metody. Wykorzystują słabo zabezpieczone okna i drzwi, często pozostawione również otwarte poprzez roztargnienie właścicieli. Ich łupem najczęściej padają pieniądze, biżuteria, drobna elektronika. Okradane są też samochody. Przestępcy szukają słabo zabezpieczonych pojazdów, wykorzystują specjalne technologie, takie jak waliszki do skanowania kluczyków. W ten sposób dostają się do środka auta, mogą ukraść cenne przedmioty w nim pozostawione lub auto.

Oszustwa

W tym przypadku kreatywność przestępców nie zna granic. Po dobrze nam znanych metodach kradzieży „na wnuczka” lub „na policjanta” modny jest sposób „na urzędnika”, który rzekomo dokonuje inspekcji domu przed uzyskaniem świadectwa energetycznego. W zależności od tego, jaki przyjmie wariant działania, albo próbuje wymusić pieniądze za pozytywne załatwienie sprawy w urzędzie, albo po prostu dokonuje swoistej inspekcji domu w celu oceny potencjalnych łupów. Powinniśmy pamiętać o zasadzie ograniczonego zaufania wobec nieznanych nam osób.

Nie należy również zapominać o cyberprzestępcach, którzy chcą wykraść nasze dane dostępne, np. hasło do konta bankowego. W tym przypadku również powinniśmy zachowywać szczególną ostrożność, gdy ktoś prosi nas o podanie danych lub jeśli otrzymujemy SMS-a lub e-mail z linkiem, w który mamy kliknąć. Wiadomości te często są ludzko podobne do otrzymywanych z dobrze nam znanych instytucji, takich jak banki, jednak nie mają z nimi nic

wspólnego, a kliknięcie w taki link może nas drogo kosztować. O ile w przypadku próby kradzieży danych lub oszustwa „na wnuczka” najlepszym sposobem obrony jest zachowanie czujności, o tyle w przypadku fizycznych kradzieży konieczne jest wprowadzenie odpowiednich środków bezpieczeństwa i procedur.

Większe możliwości w tym przypadku mają duże firmy dysponujące odpowiednimi budżetami na zaawansowane systemy zabezpieczeń oraz ochronę fizyczną. W przypadku małych przedsiębiorstw i gospodarstw domowych nakłady te nie zawsze się kalkuluje lub właściciele nie znają wszystkich możliwych metod.

Samorządy się chronią i bronią

Samorządy coraz częściej budują zintegrowane miejskie centra monitoringu obejmujące zasięgiem miejsca uznawane za niebezpieczne, dzięki czemu mogą szybko dostrzec potencjalne zagrożenie i wysłać we wskazane miejsce odpowiednie służby. Uzupełnienie systemu monitoringu wizyjnego o głośniki i reflektory powoduje, że interwencji można się podjąć zdalnie, błyskawicznie reagując na sytuację. Świetnymi przykładami takich rozwiązań są system monitoringu miejskiego Straży Miejskiej w Łodzi z 915 kamerami czy Katowicki Inteligentny System Monitoringu i Analizy obejmujący aktualnie 339 kamer. Dzięki nim liczba kradzieży i przestępstw

» Tylko na Mazowszu do końca listopada 2022 r. policja odnotowała 874 włamania do mieszkań. To o ponad 40% więcej niż rok wcześniej i aż o 75% więcej niż w roku 2020. «





w tych miastach wyraźnie spada. I chociaż pojawia się wiele głosów na temat tego, że w ten sposób pozbawia się obywateli prywatności, nie jest to duża cena za poprawę bezpieczeństwa.

Należy dodać, iż w ostatnich latach wiele służb zaczęło również stosować technologie informatyczne i sztuczną inteligencję w celu poprawy swojej skuteczności. Przykładami takich rozwiązań są systemy monitoringu i analizy danych, systemy wczesnego ostrzegania przed zagrożeniami oraz narzędzia do automatycznego wykrywania podejrzanego lub odbiegającego od normy zachowania.

Warto również zaznaczyć, że służby stojące na straży bezpieczeństwa często współpracują ze sobą, wymieniając informacje i koordynując swoje działania w celu skuteczniejszego zwalczania zagrożeń. Współpraca ta może mieć charakter krajowy, ale także międzynarodowy, co jest szczególnie ważne w przypadku walki z międzynarodową przestępczością zorganizowaną i terroryzmem. W przypadku działań krajowych służby często wymieniają informacje i współpracują ze sobą w celu śledzenia podejrzanych osób lub grup przestępczych. Wraz z szybkim rozwojem technologii koordynacja działań między służbami stała się mniej skomplikowana. Wiele krajów tworzy specjalne systemy informatyczne, które umożliwiają wymianę informacji w czasie rzeczywistym. Pozwala to na zdecydowanie sprawniejsze

i szybsze działanie oraz zapobiega występowaniu kolejnych przestępstw. Koordynacja działań między służbami jest kluczowa dla zapewnienia bezpieczeństwa obywatelom na poziomie zarówno krajowym, jak i międzynarodowym. Wymaga jednak wielu wysiłków i stałego rozwoju w dziedzinie technologicznej i organizacyjnej.

Jak się chronić?

Montaż systemu alarmowego i monitoringu wizyjnego okaże się bardzo przydatny, jako że może odstraszyć potencjalnych złodziei. Pomocne są też dobre kontakty z sąsiadami. Któż lepiej przypilnuje dobytku podczas naszej nieobecności niż sąsiad.

Realizację powyższych punktów ułatwia zaawansowana technologia. Odpowiednio zaprojektowane systemy zabezpieczeń mogą znacząco zwiększyć poziom bezpieczeństwa.

Montaż monitoringu wizyjnego powinien być standardem w każdym przedsiębiorstwie. W zależności od wielkości chronionej powierzchni i miejsca montażu wybieramy kamery o odpowiedniej rozdzielczości oraz o szczególnych właściwościach. W przypadku ujęcia sprawcy informacje zapisane w pamięci systemów wizyjnych stanowią doskonały materiał dowodowy. Ponadto systemy monitoringu wizyjnego z wbudowaną sztuczną inteligencją znacząco ułatwiają pracę operatorom i przyspieszają podjęcie przez nich decyzji. Wtargnięcie człowieka, parkowanie pojazdów w strefie niedozwolonej, wejście do strefy zdefiniowanej lub wyjście z niej – takie informacje operator otrzymuje w czasie rzeczywistym. W sklepach, które zdecydowały się na uruchomienie kas samoobsługowych, można zastosować specjalne systemy wizyjne rejestrujące nazwę skanowanego produktu, jego cenę i porównując ją z informacjami zapisanymi w bazie. Gdy występuje niezgodność, uruchamiają alarm.

W przypadku mniej wyrafinowanych prób kradzieży przydatna będzie technologia RFID, która jest rozwiązaniem pozwalającym na bieżące monitorowanie faktycznych stanów magazynowych asortymentu oraz ich lokalizacji w określonych strefach. Podczas próby kradzieży bramka poinformuje nas o tym. Za pomocą tej technologii można również błyskawicznie przeprowadzać remanenty oraz poprawić szybkość i dokładność dostaw, co ma znaczenie ekonomiczne.

Należy jednak pamiętać, że nawet dobry system się nie sprawdzi, jeśli nie będzie go obsługiwał odpowiednio wyszkolony pracownik. To w końcu człowiek w sytuacjach kryzysowych musi ocenić sytuację, przeanalizować wszystkie informacje i podjąć działania często decydujące o czymś zdrowiu lub życiu. Dlatego tak bardzo potrzebni są kompetentni operatorzy, umiejący obsługiwać coraz bardziej rozbudowane platformy zabezpieczeń. Aby ograniczyć straty, należy inwestować w nowe technologie i szkolenia pracowników, co zapewni odpowiedni poziom bezpieczeństwa. I to w takim hybrydowym modelu jest przyszłość. ●



Tomasz Grzelak

Security manager z wieloletnim doświadczeniem w międzynarodowym biznesie. Specjalizuje się w obszarze handlu i logistyki, z osiągnięciami w innowacyjnych projektach technologicznych i organizacyjnych. Specjalista w zakresie negocjacji, zarządzania oraz bezpieczeństwa fizycznego i korporacyjnego. CEO w Stay Safe Poland / Security Inspector w DPD Polska.

Jako wynik zacieśniających się relacji pomiędzy Polską a Koreą Południową, szczególnie w obszarach bezpieczeństwa



Megavision Technology ogłasza premierę na polskim rynku

KAMER IP KLASY HIGH-END

docenionych i wykorzystywanych powszechnie od lat na rynku USA i innych państw NATO

Co mogą robić firmy, np. sklepy różnej wielkości lub zakłady produkcyjne

- zidentyfikować obszary narażone na największe straty,
- wykonać dogłębną analizę, gdzie i kiedy dochodzi do strat,
- wytypować najlepsze i optymalne sposoby przeciwdziałania stratom i wdrożyć je,
- monitorować efektywność systemów zabezpieczeń i w razie potrzeby wprowadzać korekty.

Kamery wieloprzetwornikowe

Wprowadzenie kamer wieloprzetwornikowych zmieniło funkcjonowanie monitoringów miejskich, jedna taka kamera dysponuje bowiem znaczenie większym polem widzenia w porównaniu z kamerami jednoprzetwornikowymi. Wcześniej zapewnienie 360° pokrycia sceny wymagało instalacji czterech kamer, obecnie ten sam efekt można osiągnąć za pomocą jednego urządzenia.

Jan T. Grusznic, a&s Polska

Rynek kamer wieloprzetwornikowych rozwijał się w ciągu ostatnich lat dwukrotnie szybciej niż rynek kamer PTZ, a prognozy są takie, że w latach 2023-2029 będzie rosnać w tempie 4,7% CAGR (wg danych Market intelligence). Skąd takie zainteresowanie multisensorymi? Z prostej przyczyny – mogą one radykalnie zwiększyć świadomość sytuacyjną, dostarczając obrazy o względnie wysokiej szczegółowości rozległego obszaru. Jedna kamera wieloprzetwornikowa może zastąpić wiele kamer konwencjonalnych, znacznie obniżając koszt związany z zakupem wielu kamer, ich instalacją, koniecznością zadbania o infrastrukturę i zakupem licencji. W monitoringu wizyjnym rozwiązania te odgrywają kluczową rolę w nadzorowaniu obszarów rozległych, a dzięki algorytmom sztucznej inteligencji kamery te staną się jeszcze wydajniejsze i bardziej uniwersalne.

Czym jest kamera wieloprzetwornikowa?

Kamery wieloprzetwornikowe rozwiązują wiele problemów związanych z dozorem wizyjnym, z którymi borykają się specjaliści ds. bezpieczeństwa. Proces planowania już średniej instalacji może się skomplikować pod względem okablowania, punktów montażu,

urządzeń aktywnych sieci i dostępnych w nich portów, a także innych wymagań instalacyjnych. Jedną z zalet kamer wieloprzetwornikowych jest możliwość uproszczenia procesu projektowania i budowy przy jednoczesnym zastosowaniu wielu najlepszych praktyk w celu zwiększenia pokrycia szerokiego obszaru i zminimalizowania kosztów sprzętu, gdyż multisensory w jednej obudowie mieszczą kilka kamer o rozdzielczości na ogół od full HD do 4K, co pozwala na ogólny dozór bez martwych punktów.

Koncepcja tych urządzeń szybko ewoluowała i dzisiaj w zależności od budowy wyróżniamy:

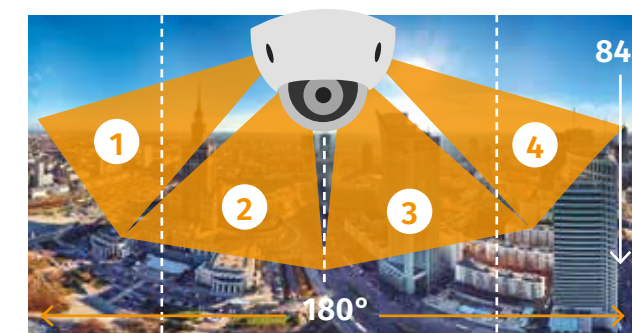
1. Kamery wielokierunkowe – wewnętrzne ułożenie modułów przetworników z układami optycznymi umożliwia niezależną pracę. To od tego rozwiązania rozpoczęła się ewolucja kamer wieloprzetwornikowych. Obecne urządzenia zapewniają już zdalne pozycjonowanie ogniskowej, ustawianie ostrości, położenia przetwornika (0°, 90°, 180°, 270°), a nawet ustawienie głowicy, dzięki czemu instalacja przebiega sprawnie, bez konieczności ręcznego ustawiania każdego modułu. Wykorzystanie dostarczonych w kamerze obiektywów zmiennoogniskowych, zapewniających kilkukrotne zbliżenie optyczne, pozwala na uzyskanie większej szczegółowości wybranego obszaru sceny za pomocą jednego

modułu, podczas gdy pozostałe kontynuują ogólny dozór. Kamery sprawdzają się najczęściej w dozorcze skrzyżowań i obserwacji otoczenia rogów budynków, jak również strefy perymetrycznej w „rogach” działki.



Rys. 1. Przykład kamery wieloprzetwornikowej wielokierunkowej

2. Kamery panoramiczne – każdy z układów optycznych współdziała z pozostałymi. Obrazy z przetworników nieznacznie nakładają się na siebie, a następnie są „zszywane” (stitching) przez wbudowane w kamerę oprogramowanie, co daje jednolity panoramiczny widok z większą liczbą szczegółów niż dostarczany przez kamery typu „rybie oko”. Konstrukcja kamery nie zakłada możliwości ustawienia ogniskowej lub korekty ostrości, jak w przypadku kamer wielokierunkowych. Moduły optyczne są umieszczone na wspólnej szynie montażowej, zapewniając zsynchronizowaną zmianę położenia góra-dół, dzięki czemu efekt łączenia obrazów z przetworników pozostaje niezauważalny. Kamery tego typu są idealne do obserwacji ulic, deptaków, placów, parków, terenów dworców i portów.



Rys. 2. Przykład kamery wieloprzetwornikowej panoramicznej

3. Panomera® – jest rozwiązaniem oferowanym tylko przez jedną firmę, ale na tyle innowacyjnym, że nie sposób go pominąć. W przeciwieństwie do ww. rozwiązań to urządzenie składa się z wielu kamer o różnych ogniskowych ułożonych w strukturze macierzowej. Dzięki temu urządzenie rejestruje obszary tła obrazu i znajdujące się w średniej odległości od miejsca montażu z taką samą rozdzielczością jak scenę na pierwszym planie. Obraz w tym przypadku jest łączony za pomocą zewnętrznego oprogramowania, a potrzebna liczba licencji w oprogramowaniu VMS równa jest liczbie przetworników znajdujących się w zespole optycznym.

Współczesne kamery wieloprzetwornikowe zapewniają doskonałą świadomość sytuacyjną, tak oczekiwaną w systemach dozoru wizyjnego. Szerokie pole widzenia pozwala operatorom na natychmiastowe zrozumienie sceny, a możliwość przybliżenia szczegółów i nawigowania po obrazie sprawdza się w przypadku dochodzenia po zdarzeniu. Zasilone analizą obrazu opartą na uczeniu maszynowym lub sieciach neuronowych zmieniają systemy zabezpieczeń wizyjnych z rozwiązania reaktywnego na proaktywne. Mogą pomóc w wykrywaniu i ostrzeganiu operatorów o potencjalnych zdarzeniach wymagających uwagi, np. o osobach lub pojazdach przemieszczających się w zakazanej strefie, a także pomóc w skróceniu czasu reakcji i prowadzeniu dochodzeń. Możliwości są olbrzymie, a fakt, że można to wszystko zrobić z jednego punktu obserwacyjnego, również ma istotne znaczenie.

Dodatkowa korzyść – mniejszy koszt

Wykorzystanie kamer wieloprzetwornikowych otwiera drzwi do wielu korzyści związanych z obniżeniem kosztów. W monitoringu miejskim np. kamera wielokierunkowa zapewni pełne pokrycie skrzyżowania przy użyciu tylko jednego urządzenia, jednego uchwytu i jednego połączenia kablowego. Mniejsza liczba kamer przekłada się na niższy koszt całego systemu. Wymagana jest przecież mniejsza liczba przełączników sieciowych i na ogół potrzebna jest tylko jedna licencja VMS, co znacznie obniża koszty w porównaniu z użytkowaniem kilku kamer stacjonarnych pokrywających ten sam obszar. Również z powodu mniejszej liczby wymaganych urządzeń można zmniejszyć opłaty dotyczące zasilania i instalacji. Dodanie do projektu kamer wieloprzetwornikowych może być również wykorzystane do uzupełnienia istniejących modeli stałopozycyjnych i PTZ, zapewniając bardziej kompleksowy plan nadzoru ze zwiększonym pokryciem, co znacznie ogranicza liczbę martwych stref.

Równie ważną kwestią jest estetyka. Zamiast kilku kamer skierowanych w różne strony wystarczy jedna, lecz wieloprzetwornikowa. Przykładowo kamera z czterema przetwornikami może objąć zasięgiem obszar pod kątem 270° z jednym modułem optycznym skierowanym do przodu, jednym skierowanym w dół i dwoma skierowanymi na boki. W ten sposób jedna kamera zamontowana na rogu budynku może zastąpić cztery stacjonarne pokrywające to samo pole widzenia.

Ograniczenia

Kamery wieloprzetwornikowe, chociaż są idealne do nadzorowania rozległych terenów, nie do końca radzą sobie z rejestracją szczegółów. Omawiane rozwiązania są wprawdzie projektowane z przetwornikami o wysokiej rozdzielczości, co może skutecznie zwiększyć zasięg kamery do celów wykrywania i monitorowania, jednak dokładna identyfikacja i rozpoznanie są możliwe tylko w bliskiej odległości.

Większe rozdzielczości to też większy strumień danych. Choć kamera wieloprzetwornikowa to fizycznie jedno urządzenie,

to bitrate (ilość danych transferowanych przez konkretne urządzenie w przedziale czasowym – nazywany również przepływnością) należy liczyć osobno dla każdego zespołu optycznego, nie zaś dla całego urządzenia. Jest to najczęstszy błąd podczas projektowania i planowania przestrzeni dyskowej dla systemu dozoru wizyjnego wyposażonego w takie rozwiązania. Szczęśliwie tak samo jak kamery jednoprzetwornikowe, również multisensory zostały wyposażone w technologię smart kodeków, które obniżają wymagania dotyczące szerokości pasma i pojemności pamięci masowej przy niezauważalnej stracie jakości obrazu. W zależności od złożoności scen i intensywności ruchu można uzyskać do 70% oszczędności pasma. W przypadku scen bardzo intensywnych oszczędność pasma może wynieść ok. jednej trzeciej.

Większość kamer wieloprzetwornikowych zawiera funkcje analizy zawartości obrazu, przy czym tylko kilkanaście modeli może pochwalić się zastosowaniem algorytmów uczenia maszynowego lub użyciem sieci neuronowych. Wynika to z ograniczonej mocy obliczeniowej urządzeń, która jest wykorzystywana niemal w całości do przetwarzania sygnałów z kilku przetworników jednocześnie, a w przypadku kamer panoramicznych potrzebna jest jeszcze do połączenia obrazów ze sobą. Fuzja danych i ich przetwarzanie z wielu przetworników wymaga większej wydajności zarówno samego urządzenia, jak i jego oprogramowania. Ten problem nie występuje w konwencjonalnych kamerach jednoprzetwornikowych.

Standaryzacja (np. ONVIF) i możliwość dokonywania analizy przez urządzenia zewnętrzne innych producentów jest rozwiązaniem, ale niestety kosztownym. Ograniczenia techniczne ujawniają się również w częstotliwości odświeżania obrazu, nie zawsze możliwe jest uzyskanie 25 kl./s w pełnej rozdzielczości.

Istotnym ograniczeniem, zwłaszcza w dzisiejszych trudnych czasach jest fakt, że kamery wieloprzetwornikowe są droższe niż większość kamer jednoprzetwornikowych.

Podsumowanie

Kamery wieloprzetwornikowe sprzyjają obniżeniu kosztu posiadania, zwłaszcza w miejscach, gdzie do obserwacji całego terenu trzeba zastosować wiele kamer tradycyjnych. Stanowią nieocenioną pomoc w szybkiej analizie zdarzenia post factum z uwagi na szeroki kąt obserwacji. Jednak ze względu na ograniczoną moc obliczeniową tych urządzeń sprawdzają się jako uzupełnienie systemu dozoru wizyjnego, a nie jego baza. Zaletą przemawiającą za wprowadzeniem takich kamer do systemu monitoringu jest to, że zapewniają szeroki kąt widzenia, umożliwiając detekcję na krótszych odległościach w porównaniu z kamerami jednoprzetwornikowymi, nie mając sobie równych w dozorze skrzyżowań, obserwacji otoczenia rogów budynków, ulic, deptaków, placów, parków, terenów dworców i portów. ●

» Kamery wieloprzetwornikowe obniżają „koszt posiadania”, zwłaszcza w miejscach, gdzie do obserwacji całego terenu trzeba zastosować wiele kamer tradycyjnych. «

BCS



Kamera BCS-L-DMIP-4X5MWSIR3-V-A-AI2 to tak naprawdę 4 wysokiej jakości kamery zamknięte w jednej obudowie. Każda z nich może być traktowana jako osobne urządzenie, przekazując oddzielne strumienie do rejestratora. Jednak od strony instalacji traktujemy ją jako jedno urządzenie. Kamera ta pozwoli w łatwy sposób monitorować ciągi komunikacyjne w budynkach czy skrzyżowania ulic.

Więcej na <https://bcs.pl>

Parametr	Wartość
Model	BCS-L-DMIP-4X5MWSIR3-V-A-AI2
Liczba przetworników	4
Rozdzielczość przetwornika	5 Mpix
Zdalne ustawianie ostrości pozycji ogniskowej	Nie
Zakres ogniskowej	2,8 mm
Zasilanie	PoE
Analiza obrazu	Oparta na AI, każdy przetwornik może korzystać z innej analizy. Detekcja twarzy lub ochrona parametryczna: przekroczenie linii, wtargnięcie. Do 10 zasad na przetwornik.
Współpraca z PTZ	tak -ysterowanie PTZ po pojawieniu się ruchu w strefie
Wbudowane oświetlenie IR	Tak
Obserwacja (zgodnie z PN-EN 62676-4)	≤ 36m
Przeznaczenie	Dozór rogów budynków, skrzyżowań, korytarzy

Hikvision



Seria DS-2CD6D54 to 4 niezależne moduły kamerowe w jednej obudowie. Zdalna regulacja ogniskowej i ostrości, jeden adres IP, wspólny interfejs GUI, 3 sposoby zasilania, a to wszystko uzupełnione bogatym zestawem analityk obrazu. Ponadto zapis lokalny na karcie SD, funkcja zapisu awaryjnego z automatycznym przekazaniem nagrań do serwera, dwukierunkowa transmisja dźwięku, opcja interfejsu optycznego, IP67, IK10, bogaty pakiet bezpieczeństwa cybernetycznego, możliwość umieszczenia własnego logotypu na obrazie

Więcej na www.hikvision.com/pl/

Parametr	Wartość
Model	Seria DS-2CD6D54
Liczba przetworników	4
Rozdzielczość przetwornika	5 Mpix
Zdalne ustawianie ostrości pozycji ogniskowej	Tak Nie Tak
Zakres ogniskowej	2,8-12 mm
Zasilanie	12 VDC, 24 VAC, Hi-PoE
Analiza obrazu	Oparta na AI, 12 różnych scenariuszy dla każdego przetwornika
Współpraca z PTZ	TAK -ysterowanie PTZ za pomocą zdarzenia analizy obrazu
Wbudowane oświetlenie IR	TAK
Obserwacja (zgodnie z PN-EN 62676-4)	≤ 90m
Przeznaczenie	Dozór rogów budynków, skrzyżowań, terenów rozległych



Integracja systemów zabezpieczeń

Każdy użytkownik systemów zabezpieczeń jest zainteresowany zarządzaniem pracą swoich urządzeń za pomocą wspólnego oprogramowania lub aplikacji mobilnej.

Wojciech Pawlica

Bardzo często połączenie systemu alarmowego, monitoringu wizyjnego czy wideodomofonu w spójny system wiąże się z dodatkowym okablowaniem odpowiednich wejść czy wyjść, które później spełniają funkcję integracyjną. Firma Dahua Technology Poland oferuje rozwiązanie, które nie wymaga żadnego dodatkowego okablowania, a integrację zapewnia połączenie urządzeń we wspólną sieć. Integrowane są trzy oddzielne systemy:

beprzewodowy system alarmowy, system monitoringu wizyjnego oraz wideodomofon.

Beprzewodowy system alarmowy pracuje na bazie centrali ARC3000H-FW2(868). Jest to urządzenie umożliwiające zaprogramowanie do 150 czujników, 64 pilotów, 8 klawiatur, 4 repeaterów. Programowanie urządzenia jest bardzo proste, wykorzystuje się do tego aplikację DMSS. Wystarczy najpierw do aplikacji wprowadzić centralę, a następnie wszystkie kolejne urządzenia. Programowanie kolejnych urządzeń polega na zeskanowaniu kodów QR, które znajdują się na opakowaniu i urządzeniu.

Kolejnym krokiem jest wprowadzenie dwóch pozostałych podsystemów, również za pomocą tej samej aplikacji (DMSS). Po zainstalowaniu i zaprogramowaniu trzech różnych systemów zabezpieczeń można przystąpić do ich

integracji. Integracja systemów alarmowego i monitoringu wizyjnego będzie polegać na dwustronnej wymianie informacji pomiędzy systemami. Od pewnego czasu nasze rejestratory sieciowe NVR oraz hybrydowe XVR umożliwiają pracę w trybie uzbrojenia lub rozbrojenia. Tę funkcję można uruchomić za pomocą zarówno aplikacji DMSS, jak i integracji z systemem alarmowym. Przy uzbrajaniu systemu alarmowego w tryb uzbrojenia jest jednocześnie wprowadzany rejestrator.

W przypadku zastosowania kamer typu TiOC aktywuje się w ten sposób funkcjonalność audio i video (głośne i wizualne powiadomienie z kamery o naruszeniu przestrzeni, pojawienie się człowieka lub pojazdu, przekroczenie linii, wejście lub wyjście ze strefy oraz inne typy zdarzeń, które zaprogramujemy). Oczywiście w przypadku kamer nieposiadających LED-ów migających w kolorze niebiesko-czerwonym czy wbudowanego głośnika odtwarzającego dźwięk syreny lub dowolnego komunikatu można wykorzystać sygnalizator systemu alarmowego, który przy wykryciu ruchu lub innego typu analizyki powiadomi głośnym dźwiękiem i mocnym światłem stroboskopowym.

Kolejnym rozwiązaniem integrującym beprzewodowy system alarmowy z monitoringiem wizyjnym jest możliwość rozpoczęcia procesu nagrywania na rejestratorze obrazu z kamery w przypadku naruszenia któregośkolwiek z czujników w systemie alarmowym. Wszystkie powyższe rozwiązania integracji pomiędzy oboma systemami wymagają jedynie kilku kliknięć w oprogramowaniu obu typów urządzeń.

Integracja z systemem wideodomofonowym jest możliwa wyłącznie z monitorami VTH z oprogramowaniem Android. Firma Dahua ma w ofercie kilka różnych modeli takich urządzeń. W tym przypadku z poziomu monitora można uzbroić lub rozbroić system alarmowy, traktując monitor jako dodatkowy element umożliwiający taką funkcję. Monitor VTH będzie również wyświetlał zdarzenia w systemie, alarmy, awarie itp.

Integracja beprzewodowego systemu alarmowego z wideodomofonami i systemem monitoringu wizyjnego znacznie ułatwia użytkownikom korzystanie z takiego rozwiązania. •

Więcej szczegółów na stronie www.dahuasecurity.com



Dahua Technology Poland
ul. Salsy 2, Lisbon Building
02-823 Warszawa
www.dahuasecurity.com/pl

Wskazówka:
Integracja z Dahua NVR/XVR oraz monitorami VTH z Android w sieci LAN. Niezależnie od dodatkowych kodów i oprogramowania. (Dahua NVR/XVR z VTH wymagają specjalnej wersji FW).



Beprzewodowa elektroniczna kontrola dostępu

w budynkach biurowych

System elektronicznej kontroli dostępu Winkhaus blueSmart pozwala na zaawansowane zarządzanie dostępem osób do pomieszczeń w budynku.

Magdalena Madej

Zapewnia to nie tylko fizyczną ochronę pracowników i mienia, ale także zabezpiecza istotne dla funkcjonowania firmy zasoby, wrażliwe dane czy kluczową infrastrukturę.

Bezpieczny

Zarówno pracownicy, jak i inne osoby uprawnione do przebywania w budynku mają dostęp tylko do wyznaczonych przez administratora stref i pomieszczeń, zazwyczaj w przedziałach czasowych określonych do wykonania pracy. Każda operacja klucza we wkładce jest rejestrowana. Dzięki temu, jeśli ktoś podejmie próbę otwarcia pomieszczenia, do którego nie ma przyznanego dostępu, zdarzenie to zostanie odnotowane w systemie i w szczególnych przypadkach może stanowić cenną informację dla zarządu firmy. Jeżeli posiadany przez pracownika elektroniczny klucz zostanie zgubiony lub skradziony, zostaje szybko usunięty z systemu i staje się bezużyteczny. Ma to także zastosowanie w przypadku pracowników odchodzących z firmy, którzy z jakiegoś powodu nie zwrócili swojego klucza.

Cechą wyróżniającą system blueSmart jest połączenie zalet systemów mechanicznych z elastycznością zaawansowanej elektroniki. Drzwi są w pełni zaryglowane, jak w tradycyjnym zamku, a nie tylko zablokowane przez elektrozaczep. Ma to duże znaczenie zwłaszcza w przypadku drzwi zewnętrznych.

Wygodny

Właściwie skonfigurowany i wdrożony system jest wygodny i przyjazny dla użytkownika. Korzystając ze swoich uprawnień, użytkownik może – bez problemu i udziału innych osób – wejść na teren firmy oraz w czasie pracy korzystać ze wszystkich stref, pomieszczeń i urządzeń niezbędnych do jej wykonywania. Uprawnienia użytkowników mogą być łatwo modyfikowane w systemie przez administratora. W zależności od potrzeb

można je dowolnie rozszerzać lub ograniczać i konfigurować zgodnie z zaplanowanym czasem pracy.

Elektroniczna kontrola dostępu może również współpracować z innymi systemami działającymi na terenie firmy. Umożliwia to kontrolę za pomocą jednego klucza nie tylko nad otwieraniem drzwi, ale także rejestracją czasu pracy, sterowaniem windą, uruchamianiem maszyny produkcyjnej, biurowej drukarki czy nawet ekspresu do kawy. Dzięki wyposażeniu w dodatkowy transponder użytkownik może też tym samym kluczem otwierać szlabany, sterować oświetleniem czy uzbroić system alarmowy.

System blueSmart pozwala na rozszerzenie o nowe wkładki i klucze w dowolnym momencie. Może składać się nawet ze 195 tys. komponentów. W przypadku małych firm stosuje się mniejszy system blueCompact, który obejmuje maks. 25 wkładek i 99 kluczy i jest obsługiwany za pomocą aplikacji w smartfonie. Ten sam system może funkcjonować w więcej niż jednym budynku i różnych, nawet oddalonych od siebie lokalizacjach.

Łatwy w instalacji

Instalacja systemu, po wcześniejszym skonfigurowaniu zgodnie z wytycznymi inwestora, zajmuje nie więcej niż jeden dzień. Polega ona na wymianie wkładek mechanicznych w drzwiach na ich odpowiedniki elektroniczne i zamontowaniu przy wejściu czytnika lub czytników, które jako jedyne wymagają okablowania. Nie ma potrzeby prowadzenia prac remontowych ani ingerencji w ścianę budynku.

Zastosowanie systemu elektronicznego zapewnia nieograniczoną liczbę kombinacji użytkowników i ich uprawnień. W razie zagubienia lub kradzieży klucza nie ma potrzeby przeprowadzenia wymiany zamknięć w obiekcie, jedynym kosztem jest zakup nowego klucza i nadanie mu uprawnień. Dzięki połączeniu wielu funkcji w małym kluczu oszczędzamy zarówno czas, jak i pieniądze. •



Winkhaus Polska Beteiligungs
ul. Przemysłowa 1, 64-130 Rydzyna
bluesmart@winkhaus.pl
Bluesmart.winkhaus.com



Inteligentne budynki numerem 1 na rynku nieruchomości

Bezpieczeństwo budynków komercyjnych to kluczowy element zarządzania nieruchomościami. Czy inwestycja w nowoczesne systemy ochrony może podnieść wartość oferty biznesowej? W odniesieniu do *smart building* zdecydowanie tak. Co więcej, chronione w ten sposób budynki wyróżniają się na tle konkurencji.

Świadcząc usługi bezpieczeństwa, proponujemy inteligentne rozwiązania, ale ich wybór poprzedzamy analizą potrzeb, zagrożeń i ryzyka oraz możliwości wykorzystania zasobów klienta. Pozwala to optymalnie dostosować usługi i technologie oraz obniżyć koszty. Jak skutecznie zapewnić bezpieczeństwo biura lub innego budynku komercyjnego? W odpowiedzi na to pytanie prezentujemy pięć trendów wartych rozważenia.

Kontrola dostępu to zdecydowanie nr 1 na liście priorytetów zarządców. Nie oznacza tylko ograniczenia dostępu do przestrzeni biurowej, parkingowej i stanowisk pracy dla osób uprawnionych, lecz także monitoring działań użytkowników.

W Securitas systemy zabezpieczeń mają być „niewidoczne”, ale zawsze skuteczne. Ludzie dobrze czują się w środowisku, w którym ruch jest swobodny, lecz trzeba pamiętać, że dostęp do stanowisk pracy musi być pod kontrolą. W tym zakresie wykorzystujemy różne inteligentne rozwiązania, do których należy *Automatic License Plate Recognition* – system rozpoznawania tablic rejestracyjnych, systemy mobilnego dostępu oraz zabezpieczenia biometryczne. Dzięki nim uprawnione osoby mają dostęp bez konieczności stosowania kart identyfikacyjnych. Goście korzystają z usługi Securitas smartIN – łatwego w obsłudze systemu usprawniającego proces awizacji, który wysyła zaproszenia, synchronizuje terminy, powiadamia o przybyciu osób, przydziela

i rezerwuje miejsca parkingowe oraz przyznaje unikatowy kod dostępu. Gość, jeszcze przed przybyciem, otrzymuje szczegóły spotkania i w umówionym dniu po prostu wchodzi do budynku, dokładnie wiedząc, gdzie ma się udać. Awizacja w systemie Securitas smartIN oznacza też automatyczny wpis na listę ewakuacyjną budynku, co jest bardzo ważnym elementem systemu bezpieczeństwa.

Kamery i zdalny monitoring to podstawowe uzupełnienie systemów zabezpieczeń. Dojrzałość systemów analizy obrazu pozwala na wykorzystanie kamer do różnych zadań. Oprócz oczywistego dozoru w czasie rzeczywistym i wykrywania incydentów stają się elementem systemu integrującego kontrolę dostępu, system alarmowy i ochronę obwodową oraz zarządzanie miejscami parkingowymi. Wykorzystując inteligentną analizę wideo (IVA) i dozór wizyjny jako usługę (VSaaS), chronimy przed niepożądanymi incydentami i tworzymy obszary dynamicznie zabezpieczone przed zagrożeniami. Systemami zarządza Securitas Operation Center (Stacja Monitorowania Alarmów Securitas) realizująca usługi wizyjnej weryfikacji alarmów oraz zdalnych patroli monitorujących stan bezpieczeństwa obiektów w dowolnych harmonogramach czasowych.

System alarmowy jest skutecznym narzędziem do wykrywania i powiadamiania o naruszeniach. Istotne są odpowiednie zdefiniowanie i zaprogramowanie stref, a także

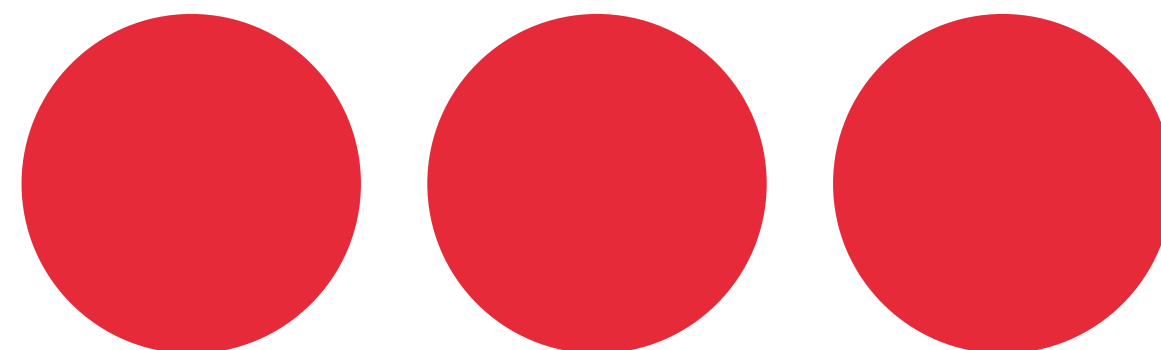
odpowiednie uzbrajanie i stały nadzór. Integracja z systemami kontroli dostępu i monitoringu wizyjnego zwiększa efektywność wykorzystania, jednocześnie sprawiając, że staje się „niewidoczny”.

Budynki komercyjne wymagają też systemów sygnalizacji pożarowej, których obsługa może być zdalna. Mobilne urządzenia dostarczają w czasie rzeczywistym informacji o zagrożeniach. To pozwala na natychmiastową (zdalną) weryfikację alarmu. Wiedza użytkowników budynków na temat procedur alarmowych jest również bardzo ważna. Polecamy wykorzystanie technologii wirtualnej rzeczywistości do szkoleń ewakuacji i przeciwdziałania zagrożeniom pożarowym.

Kolejne wyzwanie to przekazywanie przesłanych dokumentów poza godzinami pracy recepcji, które rozwiązaliśmy, wprowadzając usługę Securitas smartBOX, czyli system skrytek depozytowych. Umożliwia on całodobowy dostęp siedem dni w tygodniu do zawartości skrytek osobom uprawnionym. Wydanie przedmiotu odbywa się na podstawie unikatowej kombinacji loginu i kodu PIN. Po umieszczeniu przedmiotu w skrytce automatycznie rozpoczyna się proces przechowywania. Generowany jest kod odbioru, który zostaje wysłany odbiorcy. ●



Securitas Polska
ul. Postępu 6
02-676 Warszawa
securitas@securitas.pl





Kontrola dostępu klasy 4 według PN-EN-60839-11

Od 2014 roku obowiązuje w Polsce norma PN-EN-60839-11, której głównym celem jest pomoc w doborze odpowiedniego zabezpieczenia obiektu w zakresie kontroli dostępu w zależności od jego klasyfikacji. Norma rozróżnia cztery klasy bezpieczeństwa i dla obiektów typu: wojsko, instytucje rządowe, infrastruktura krytyczna przewidziany jest najwyższy poziom bezpieczeństwa zdefiniowany w klasie 4.

Jerzy Taczalski

Oczywiście dla tych instytucji jest to wymóg, natomiast dla innych inwestorów może być wzorcem do osiągnięcia wysokiego poziomu bezpieczeństwa. Bazując na tej normie i wstępując się w oczekiwania osób odpowiedzialnych za bezpieczeństwo w wojsku, obiektach energetycznych czy kolejowych, firma IFTER stworzyła całkowicie nowy produkt przeznaczony dla tego typu klientów. Jak każdy nasz produkt, tak i ten zaprojektowaliśmy, przykładając równą wagę do funkcjonalności i jego jakości. Dlatego nie wahamy się objąć EQU ACC400 60-miesięczną gwarancją. Model EQU ACC400 stanowi jeden z elementów nowej serii

w ramach GREENLINE, której celem będzie dostarczenie nowatorskich w tej branży rozwiązań dostosowanych do potrzeb klienta.

Należy pamiętać, że klasa 4 definiuje każdy element systemu kontroli dostępu: od czytnika, poprzez kontroler, obudowę, zasilanie i oprogramowanie. Każdy element składowy musi być stale kontrolowany i musi wykrywać wszelkie próby sabotażu czy podmiany. Dlatego dwukierunkowa komunikacja i dane są szyfrowane na każdym poziomie, począwszy od karty, poprzez czytnik, kontroler, skończywszy na oprogramowaniu nadzorczym.

W celu zapewnienia mechanicznej ochrony elektroniki kontrolerów zastosowano wytrzymałe stalowe obudowy z czujnikiem odebrania od ściany i otwarcia, dodatkowo wyposażone w szynę typu DIN-35M pozwalającą na łatwy montaż i dobór odpowiednich urządzeń. Dodatkowo kontrolery, moduły wejścia-wyjścia oraz zasilacze mają dodatkową obudowę z plastiku. W celu ułatwienia doboru urządzeń do potrzeb klienta wszystkie mają budowę modułową.

Najważniejsze są oczywiście kontrolery, które mogą obsługiwać jedno, trzy, pięć lub dziewięć przejść. Kontrolery mają wbudowany moduł Ethernet do komunikacji z innymi kontrolerami i systemem nadzorczym oraz dwa interfejsy RS485: jeden do obsługi dowolnego czytnika po protokole OSDPv2, drugi do modułów wejść/wyjść (I/O). Maksymalna długość magistrali RS485 to 1000 m. Od strony sieci Ethernet kontroler posiada zabezpieczenie przepięciowe o wartości

do 150 A(10/1000 μs) zgodnie z normą IEC 61000-4-5, a interfejsy RS485 wg tej samej normy są zabezpieczone do 600 W (10/1000 μs).

Aby uniemożliwić intruzowi podmianę lub uszkodzenie np. czujnika otwarcia, każde wejście może być zdefiniowane jako 3EOL z wykrywaniem stanów: sabotaż, rozwarcie/zwarcie, otwarcie/alarm, antimasking. Przekazniki mają wyprowadzone styki: masa, NC, NO i gwarantują aż 3 000 000 zmian stanu. Zakres temperatury pracy kontrolerów i modułów wynosi od -10°C do +40°C.

Kontroler jest zasilany w zakresie od 10 do 28 VDC, pobierając przy tym tylko 1 W energii. W celu szybkiej diagnostyki na obudowie kontrolera umieszczono diody LED prezentujące stan zasilania, alarmu, uszkodzenia, stan połączenia z Ethernetem i przez interfejs RS-485, oraz stan wejść i wyjść. Dodatkowo możliwe jest monitorowanie napięcia 230 VAC, napięcia akumulatora, napięcia zasilania kontrolera, temperatury wewnętrznej kontrolera, poziomu błędów po Ethernet i RS-485. Każda zmierzona wielkość jest przechowywana w buforze zdolnym pomieścić 1000 pomiarów, co wystarczy na pełną diagnostykę ostatniego tygodnia działania kontrolera. Dane te można pobrać do systemu nadzorczego.

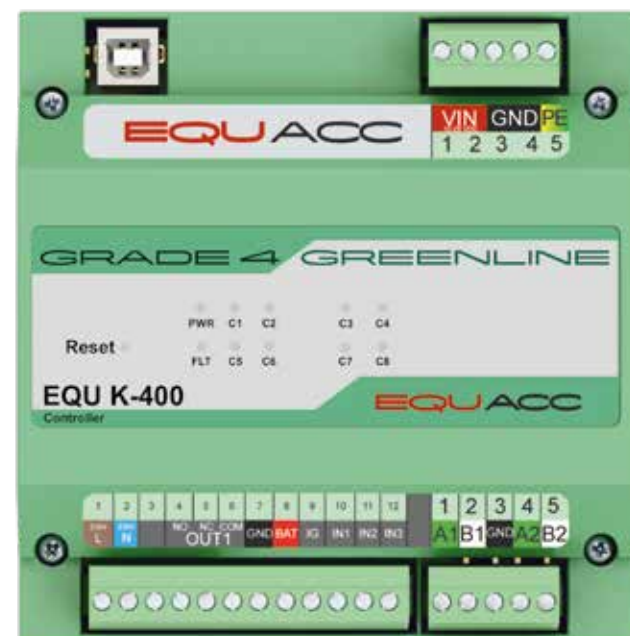
Dzięki zautomatyzowaniu procesu konfiguracyjnego EQU ACC400 proces dodawania urządzeń i zarządzania nimi został znacząco ułatwiony. Oprogramowanie nadzorcze automatycznie wykrywa i nawiązuje połączenie z nowymi kontrolerami w sieci. W celu zabezpieczenia przed cyberatakami kontroler nie reaguje na standardowe pakiety, więc inne urządzenia widzą go jako host niezidentyfikowany. Połączenie z systemem nadzorczym odbywa się tylko przez jeden port i jest aktywowane dopiero po autoryzacji oraz ustanowieniu szyfrowanego połączenia.

Każdy kontroler może obsłużyć 32 moduły wejść/wyjść, które mogą mieć w zależności od wersji: 8 wejść, 8 wyjść lub najczęściej wykorzystywany, czyli 8 wejść i 4 wyjścia. Użytkownik samodzielnie określa funkcję dla każdego z tych wejść i wyjść. Kontrolery oraz moduły zostały pozbawione przełączników mechanicznych i zworek. Cała konfiguracja odbywa się za pomocą oprogramowania konfiguracyjnego lub nadzorczego.

Pamięć i duża moc obliczeniowa pozwalają kontrolerowi nawet w podstawowej wersji przechowywać całą konfigurację oraz dane miliona kart i 500 tys. zdarzeń. Użytkownik kontroli dostępu może mieć przypisaną dowolną liczbę kart i grup dostępu (nie więcej jednak niż milion), dzięki czemu nie ma znaczenia, ile razy dana osoba zgubiła kartę lub ile razy został jej wydany jednodniowy duplikat. Wszystkie zdarzenia dotyczące konkretnej osoby zostaną przypisane właśnie do niej, niezależnie od tego, ile osób używało tej samej karty.

Każde przejście może być obsługiwane maksymalnie przez 4 czytniki, co wydaje się wystarczające nawet w przypadku montażu dwóch czytników dla przejazdu samochodów osobowych i dwóch dla ciężarówek. Nie ma przeszkód, aby przejście było obsługiwane tylko przez jeden czytnik. Mechanizm antipassback może być realizowany lokalnie przez jeden kontroler lub globalnie w ramach całej sieci kontrolerów.

Na wizualizacji opartej na planach architektonicznych mogą być prezentowane całe przejścia lub poszczególne czytniki, wejścia i wyjścia. Jeżeli standardowe funkcje kontroli dostępu będą niewystarczające, to można je rozbudować, korzystając z języka skryptowego LUA pozwalającego na powiązanie dodatkowo o stany lub sterowanie w innych integrowanych systemach.



Kontroler jednego przejścia EQU-K400

Organizacja systemu nadzorczego w EQU ACC400 została zaprojektowana na potrzeby zarządzania dużymi firmami. Do tego celu wykorzystuje zarówno bardzo rozbudowane pakiety oprogramowania w formie aplikacji pracującej pod systemem Windows, jak i na bazie przeglądark WWW pozwalających pracować z dowolnego miejsca na dowolnym systemie. Niezależnie od wielkości instalacji lokalni administratorzy mogą zarządzać systemem i uprawnieniami tylko w zakresie wcześniej nadanych uprawnień bez możliwości wprowadzania zmian wykraczających poza nie. Ułatwieniem w zarządzaniu jest integracja z usługą serwerową systemu Windows – *Active Directory*. Zatrudniona osoba automatycznie pojawia się w EQU ACC400 z opisem wymaganego zakresu dostępu. Administratorowi pozostaje jedynie zatwierdzenie dostępu do przejść. W przypadku odejścia pracownika jego uprawnienia są automatycznie blokowane. Wydawanie kart również zostało zautomatyzowane, ponieważ można je drukować bezpośrednio z oprogramowania nadzorczego wg szablonów. Automatyczne pobieranie zdjęć z aparatu fotograficznego upraszcza pracę.

Oprogramowanie nadzorcze EQU ACC400 ma bardzo rozbudowaną funkcjonalność rejestracji czasu pracy w pełni zaspokajającą potrzeby firmy. Dodatkowo klient może skorzystać z mechanizmu automatycznej awizacji gości z przesyłaniem do nich kodów QR w celu np. wjazdu na parking firmowy.

System kontroli dostępu EQU ACC400 jest bardzo nowoczesny w warstwie sprzętowej i oprogramowania ułatwiającego konfigurację, zarządzanie i diagnostykę bieżącą, opartą na najnowszej technologii informatycznej z zaawansowanym systemem integracyjnym, z wizualizacją włącznie.

Staranność wykonania tego produktu w 100% spełnia wymagania normy PN-EN-60839-11 w klasie 4, pozwalając na bardzo skuteczne zabezpieczenie obiektów potrzebujących takich rozwiązań. ●



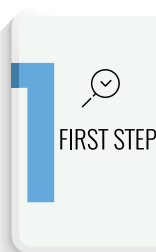
IFTER Jerzy Taczalski
21-025 Niemce
Wola Niemiecka 78c
www.ifter.com.pl



Wybór właściwego systemu zarządzania szafkami dla pracowników i dostosowanie go do potrzeb organizacji to kluczowe aspekty, by spełniał oczekiwania i był wygodny, ale także zgodny z przepisami.

Aby osiągnąć najlepsze efekty, należy wyjść poza kwestię przechowywania jedynie rzeczy osobistych. Obecnie środowiska pracy stały się bardzo dynamiczne, dlatego jest to właściwy moment, by zastanowić się nad specyfiką korzystania z przestrzeni biurowej.

Na co zwrócić uwagę przy wyborze systemu zarządzania szafkami, aby spełniał potrzeby? Pomocne będzie sześć kroków.



DO CZEGO BĘDĄ SŁUŻYŁY SZAFKI?

Po pierwsze należy zastanowić się, do czego służyć lub mogą służyć szafki. Oto cztery najpopularniejsze zastosowania zabezpieczonych skrytek w systemie zarządzania szafkami:

- bezpieczne przechowywanie rzeczy osobistych;
- bezpieczne przechowywanie rzeczy firmowych, np. dokumentów zawierających poufne dane, leków, materiałów potrzebnych do pracy zespołom;
- zarządzanie zasobami, takimi jak laptopy i inne urządzenia mobilne, sprzęt medyczny czy narzędzia budowlane. Dzięki odpowiedniemu systemowi zarządzania szafkami nie trzeba wyznaczać pracowników do wydawania i przyjmowania takich sprzętów;
- punkt odbioru, np. dla kurierów, serwisu informatycznego, przesyłek podejmowanych lub zdawanych poza godzinami pracy.



KTO BĘDZIE KORZYSTAŁ Z SZAFEK?

Gdy już wiesz, do czego będą służyły szafki, należy określić, kto będzie z nich korzystał. Szczegółowa analiza pozwoli podzielić użytkowników na grupy: pracowników, podwykonawców i gości. Analiza powinna być precyzyjna, uwzględniająca potrzeby poszczególnych grup. Aby ustalić te potrzeby, pomocne będą odpowiedzi na pytania: Czy użytkownicy danej kategorii będą przebywać w jednym miejscu, czy będą się przemieszczać? Co mogą ze sobą przynieść? W jakie dni będą potrzebować szafek? Czy będą się przebierać? I jedno z ważniejszych, czy mają specjalne potrzeby w zakresie dostępu ze względu np. na niepełnosprawność ruchową.



W JAKI SPOSÓB SZAFKI BĘDĄ UŻYWANE?

W kolejnym kroku należy się zastanowić, w jaki sposób szafki będą wykorzystywane przez poszczególne osoby w różnych sytuacjach.

Szafki indywidualne czy rotacyjne? Ważnym aspektem przed wyborem systemu zarządzania szafkami jest to, czy każda osoba będzie mieć własną szafkę, czy szafki będą wykorzystywane elastycznie.

Całodobowe czy o ograniczonej dostępności? Innym sposobem na zminimalizowanie liczby potrzebnych szafek jest rezygnacja z udostępniania ich w trybie 24/7. Zamiast tego można ograniczyć użytkownikowi dostęp do szafki, by mógł z niej korzystać w określonym czasie, np. tylko podczas swojej zmiany.

Zastosowanie niestandardowe. Należy pamiętać o wyjątkach od ustalonych reguł. Dobrą praktyką jest przeznaczenie 80% szafek do użytku standardowego, a pozostałe 20% na specjalne wymagania i wyjątkowe okoliczności.

Gdzie będą stały szafki? Należy rozważyć, czy szafki i inne zamknięte schowki będą się znajdowały w jednym miejscu, czy w różnych lokalizacjach. W tym drugim przypadku pozostaje do ustalenia jeszcze jedna kwestia – czy we wszystkich miejscach będą obowiązywać takie same zasady.



W JAKI SPOSÓB SZAFKI ZOSTANĄ ZABEZPIECZONE?

Wygoda nie jest oczywiście jedynym czynnikiem, który należy wziąć pod uwagę przy podejmowaniu decyzji. Równie ważne jest zabezpieczenie, dlatego należy się upewnić, że wybrany system zarządzania szafkami zapewnia odpowiedni poziom bezpieczeństwa. Nowoczesny system zarządzania szafkami działa w wewnętrznej sieci IP, zapewniając elastyczność i funkcjonalność. Wykorzystuje zamki elektroniczne, więc użytkownicy mogą otwierać i zamykać szafki lub schowki za pomocą kart dostępu, breloków czy przepustek. Bardziej zaawansowane systemy umożliwiają również dostęp i zabezpieczenie przestrzeni do przechowywania z użyciem technik biometrycznych bądź wirtualnych poświadczeń w smartfonie lub wydrukowanego kodu QR. Jeżeli wybór padnie na nowoczesny system oparty na IP, należy zadbać o zabezpieczenie zarówno platformy, jak i poszczególnych zamków. Platforma musi być odporna na ataki cybernetyczne i próby przejścia przez hakerów. Należy też się upewnić, że każdy zamek jest odporny na próby sabotażu i ma czujnik manipulacji.

System zarządzania szafkami Nedap idzie o krok dalej, umożliwiając ustawienie zamków w trybie transparentnym. Dzięki temu klucze deszyfrujące nie są przechowywane w zamkach, w związku z tym są trudno dostępne dla hakerów.



DODATKOWE KORZYŚCI

Gdy znasz już oczekiwania wobec systemu zarządzania szafkami, musisz się zastanowić, jakie funkcje pozwolą spełnić te cele i umożliwią uzyskanie dodatkowych korzyści. Integracja z kontrolą dostępu wpływa na znaczne podniesienie poziomu bezpieczeństwa oraz efektywność i wygodę. System można np. ustawić tak, by dana osoba mogła korzystać z szafki tylko wtedy, gdy przebywa na terenie budynku. Jeżeli np. czyjś dostęp do budynku zostanie zablokowany, można natychmiast (automatycznie) zablokować także jego szafkę.

Zdalne i centralne zarządzanie. Administrowanie dużą liczbą szafek i miejsc do przechowywania bywa czasochłonne. Zdalne i centralne zarządzanie znacznie je upraszcza, usprawnia jego funkcjonowanie i zwiększa efektywność. Najwygodniejsze jest sterowanie za pomocą urządzenia mobilnego.

» Po pandemii nastąpiło wiele zmian w modelach pracy w nowoczesnych przestrzeniach biurowych. Jedną z nich jest mniejsza liczba biurek niż pracowników i zwiększenie zapotrzebowania na szafki, w których pracownicy mogą przechowywać swoje rzeczy. Zmienił się także sposób wykorzystywania szafek. «

Anna Twardowska,
Regional Sales Manager Central & Eastern Europe,
Nedap Security Management

Integracja z innymi systemami, takimi jak system kadrowy, obsługi gości i zarządzania obiektami oznacza wygodę przydzielania dostępu do szafek i schowków według roli każdej osoby, działu, schematu zmian, długości umowy i innych kryteriów.

Dane i raportowanie. System zarządzania szafkami, który jest wyposażony w zaawansowane funkcje śledzenia i raportowania, może generować raporty służące m.in. do pozyskania informacji, kto i kiedy korzystał z danej szafki, a także analizy wykorzystania szafek.



PRZYGOTUJ LISTĘ WYMAGAŃ

Na ostatnim etapie należy opracować listę oczekiwań wobec systemu zarządzania szafkami. Tworząc plan wymagań wobec potencjalnych dostawców, należy dokładnie określić oczekiwania, pozostając jednak otwartym na sugestie.

System zarządzania szafkami to inwestycja długoterminowa, która powinna zaspokoić bieżące i przyszłe potrzeby organizacji. Bardzo ważne, aby każdy aspekt używania szafek poddać starannej analizie. Doskonałym sposobem na przegląd i weryfikację systemów zarządzania szafkami mogą być np. narzędzia do wizualizacji w 3D. Dzięki nim jeszcze przed dokonaniem ostatecznego wyboru można sprawdzić, jak dany system sprawdzi się w organizacji.

W przypadku pytań dotyczących zarządzania szafkami lub wsparcia przy wyborze czy projektowaniu systemu zapraszamy do kontaktu. •

 **Nedap Security Management**
al. Niepodległości 18
02-653 Warszawa
www.nedapsecurity.com/pl/



Realizacja Varso Tower – najwyższego budynku w Unii Europejskiej



O realizacji instalacji w kompleksie Varso Place opowiadają: Kamil Legard, prezes Zarządu, i Mikołaj Lepoew, dyrektor finansowy firmy uruchomienia.eu.

Jaka była/jest Państwa rola w projekcie Varso Place?

Firma uruchomienia.eu jest jednym z podmiotów, który odpowiada za projekty, montaż i serwisowanie instalacji technicznych w kompleksie Varso Place, zapewniając tym samym bezpieczeństwo i funkcjonalność budynków. W przypadku projektu dla najwyższego budynku w Polsce, czyli Varso Tower, którego scenariusz pożarowy liczy ponad 600 stron, wdrożenie systemu bezpieczeństwa pożarowego stanowiło bardzo ambitne wyzwanie. Realizacja obejmowała instalację m.in. 33 central CSP/CSUP Integral, ok. 25 tysięcy czujek pożarowych, ok. 4 tysięcy modułów kontrolno-sterujących, ok. 350 czujek zasysających dymu, systemu integrującego SIS-Fire, 2 systemów wizualizacji SecoLOG IP. To wszystko jest potrzebne, aby jak najlepiej wykorzystać potencjał oprogramowania przy zminimalizowaniu ryzyka popełnienia błędu ludzkiego, na który przy obiektach IK nie możemy sobie pozwolić.

O REALIZACJI:

Varso Place to kompleks trzech budynków biurowo-usługowych o powierzchni najmu 140 tys. m², usytuowanych w centrum Warszawy, w bezpośrednim sąsiedztwie Dworca Centralnego. Jeden z obiektów, monumentalny Varso Tower o wysokości 310 m, jest najwyższym budynkiem w Unii Europejskiej. Wysokościowiec ma 4 kondygnacje podziemne, 53 kondygnacje nadziemne i taras widokowy na wysokości 230 m.

O FIRMIE:

Firma uruchomienia.eu to autoryzowany Partner Schrack Seconet Polska, wykonawca instalacji teletechnicznych w najwyższym obiekcie w Unii Europejskiej. Powstała w 2014 r. firma świadczy profesjonalne usługi w branży instalacji teletechnicznych. Zapewnia kompleksową obsługę w zakresie projektowania, doradztwa, wykonawstwa, serwisowania i modernizacji instalacji niskoprądowych. Wykonuje projekty i instalacje systemów sygnalizacji pożaru, gaszenia gazem lub aerozolami, okablowania strukturalnego oraz systemów kontroli dostępu. Zapewnia funkcjonowanie instalacji w budynkach biurowych, zakładach produkcyjnych i halach magazynowych.

Co sprawiło, że to właśnie firma Schrack Seconet stała się partnerem przy realizacji tego projektu?

Nasza współpraca z firmą Schrack Seconet trwa dziewięć lat. Jakość i stabilność, jaką oferuje, okazały się nieporównywalnie wyższe niż to, co proponują inni producenci. Wysokie standardy i profesjonalizm sprawiły, że nie mieliśmy wątpliwości co do systemu, który powinien być zainstalowany przy realizacji tak złożonego projektu, jakim jest Varso Place.

Schrack Seconet jest głównym dostawcą urządzeń w zakresie instalacji sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi. Są to systemy najwyższej jakości, które zapewniają niezawodność realizowanych przez nas instalacji. Są bardzo dobrze zaprojektowane, a ich wyróżnikiem są m.in. ogromna elastyczność, możliwość skalowania i nieosiągalna przez innych producentów możliwość programowania.

Jakie wyzwania stały przy realizacji projektu najwyższego biurowca z Polsce?

Ze względu na lokalizację Varso Place w ścisłym centrum miasta największym wyzwaniem była logistyka. Dostawy materiałów wymagały awizowania często z dwutygodniowym wyprzedzeniem i dokładnością do 5 minut. W pierwszej fazie budowy obiektu transport materiałów odbywał się windami elewacyjnymi, rozbudowywanymi stopniowo wraz z budynkiem, aż do około 200 m nad powierzchnią terenu. Wszystkie elementy ruchome, nawet klucze, musiały być w takich warunkach odpowiednio zabezpieczone i przypięte do elementów stałych.

Duże wyzwanie stanowiła instalacja na wszystkich trzech tarasach systemu wczesnego ostrzegania przed burzą, zintegrowanego z systemem sygnalizacji pożarowej. Jest to najwyżżej położony system teletechniczny w Europie.

Dla zapewnienia najwyższego poziomu bezpieczeństwa pożarowego w obiekcie został wdrożony zintegrowany system bezpieczeństwa pożarowego zarządzany przez system integrujący urządzenia przeciwpożarowe SIS-FIRE. Instalacja realizuje wymagane funkcje

wczesnej detekcji pożaru i sterowania urządzeniami przeciwpożarowymi zgodnie ze scenariuszem pożarowym przez spójny certyfikowany system sygnalizacji pożarowej i sterowania urządzeniami przeciwpożarowymi Integral EvoxX.

Ścisła współpraca z SIUP SIS-FIRE zapewnia aktywne wsparcie dla operatora w zakresie lokalizacji miejsca pożaru, wyświetlenia instrukcji postępowania oraz możliwości ręcznego sterowania urządzeniami automatyki pożarowej. Zintegrowany system bezpieczeństwa pożarowego zapewnia w czasie pożaru maksymalne wsparcie dla personelu ochrony i kierującego działaniami ratowniczymi.

Jak przebiegała współpraca z firmą Schrack Seconet?

Wiemy z doświadczenia, że urządzenia firmy Schrack Seconet charakteryzują się znakomitą jakością, która spełnia najwyższe standardy, a oferta produktowa jest nieporównywalnie lepsza od konkurencji. Obsługa Schrack Seconet jest kompetentna i profesjonalna. Do tego dochodzi świetna obsługa posprzedażowa. Pracownicy prezentują indywidualne podejście do klienta, z zadań wywiązują się terminowo i zgodnie z ustaleniami. Odpowiedzialność, rzetelność, sprawne działanie i słuszenie pomocą sprawiają, że nasza współpraca przebiega wzorcowo.

Z odpowiednim partnerem biznesowym nasz zespół sprostął wyzwaniom i wykonał instalację m.in. czujek zasysających dymu w szybie windowym o wysokości 200 m, instalację 300 km kabla pożarowego, zaawansowane układy sterowania automatyką pożarową z tysiącami modułów wejścia/wyjścia. A zespół w pewnym momencie składał się z przeszło 100 osób na jednej budowie.

Naszym zdaniem najważniejsze w życiu jest zachowanie równowagi, tzw. *work-life balance*. Wszystko się udało i teraz mamy czas... na odpoczynek. Do kolejnej inwestycji, tym razem w Berlinie. ●



Schrack Seconet Polska
ul. A. Branickiego 15,
02-972 Warszawa
www.schrack-seconet.pl

Efekt tak dużej inwestycji przeszedł nasze najśmielsze oczekiwania i dał nam ogromną radość i satysfakcję.





Systemy transmisji alarmów pożarowych stanowią istotny element ochrony przeciwpożarowej budynków i umożliwiają szybką reakcję służb ratowniczych na występujące w budynkach zagrożenia pożarowe. Ich stosowanie podlega wielu rygorom formalnym, technicznym i organizacyjnym. Ich celem jest zapewnienie wysokiej sprawności i funkcjonalności systemów transmisji alarmów pożarowych (STAP) oraz ich odporności na różnego rodzaju zakłócenia i warunki środowiskowe, jakie mogą wystąpić w miejscu ich pracy/stosowania.

Grzegorz Mroczko

Ochrona przeciwpożarowa budynków

Systemy transmisji alarmów pożarowych

S trażacy tym szybciej dotrą do budynku, im we wcześniejszej fazie będzie pożar, z którym będą musieli się zmierzyć. Ma to istotne znaczenie z punktu widzenia zaangażowania sił i środków niezbędnych do uzyskania kontroli nad zdarzeniem, a następnie jego likwidacji oraz ograniczenia strat. Zadaniem systemu transmisji alarmów pożarowych jest automatyczne przekazanie informacji o zdarzeniu pożarowym z budynku nadzorowanego, przez system sygnalizacji pożarowej (SSP), do stanowiska kierowania komendy powiatowej lub komendy miejskiej Państwowej Straży Pożarnej. Ich stosowanie umożliwia szybkie zadysponowanie strażaków do prowadzenia działań ratowniczo-gaśniczych w budynku.

STAP jest zbudowany z dwóch głównych elementów:

- nadajnika przesyłającego alarm o zdarzeniu pożarowym zainstalowanego w budynku,
- stacji odbiorczej alarmów pożarowych zainstalowanej w komendzie powiatowej lub jednostce straży pożarnej.

Urządzenie do transmisji alarmów pożarowych (UTAP) najczęściej jest zintegrowane z urządzeniem do transmisji sygnałów uszkodzeniowych (UTSU). Razem jest to urządzenie do transmisji alarmów pożarowych i sygnałów uszkodzeniowych (UTAPiSU).

W odróżnieniu od informacji o zdarzeniu pożarowym sygnały uszkodzeniowe są przesyłane nie do SOAP, lecz to do stacji odbiorczej sygnałów uszkodzeniowych (SOSU), zainstalowanej w firmie świadczącej usługi monitoringu pożarowego.

Konstrukcja UTAPiSU nie podlega standaryzacji. Na rynku znajdują się zatem urządzenia różniące się kształtem, wymiarami i interfejsem.

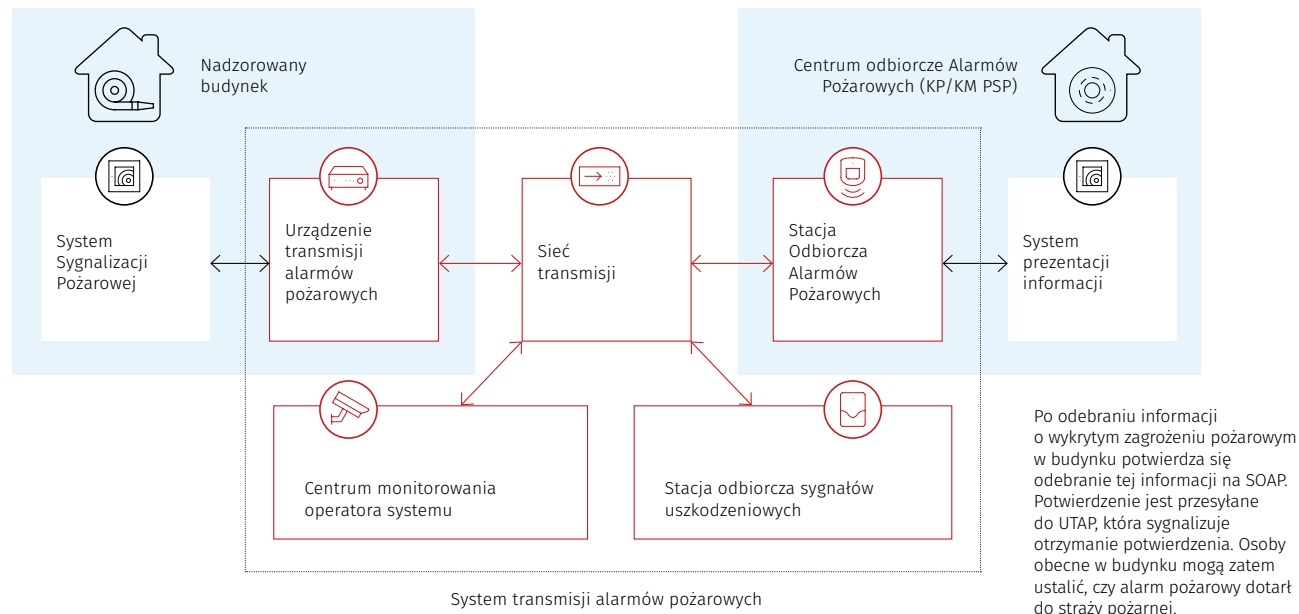
Instalacją, funkcjonowaniem, konserwacją i nadzorem nad systemami transmisji alarmów pożarowych zajmują się firmy usługowe, u których właściciele lub zarządcy budynków wykupują usługę transmisji alarmów pożarowych zwaną potocznie usługą monitoringu pożarowego.

Obowiązek ustawowy

Obowiązek instalacji systemów transmisji alarmów pożarowych podłączonych do komend PSP w obiektach, budynkach użyteczności publicznej został zapisany w Ustawie z 24 sierpnia 1991 r. o ochronie przeciwpożarowej (tj. Dz.U. 2022 poz. 2057). Mówi o tym także § 31 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 nr 109 poz. 719 z późn. zm.). Przepisy te wskazują obowiązek podłączania wybranych obiektów z KP/KM PSP: *Właściciel, zarządca lub użytkownik obiektu, o którym mowa w art. 5 ustawy z 24 sierpnia 1991 r. o ochronie przeciwpożarowej, uzgadnia z właściwym miejscowo komendantem powiatowym (miejskim) Państwowej Straży Pożarnej sposób połączenia urządzeń sygnalizacyjno-alarmowych systemu sygnalizacji pożarowej z obiektem komendy Państwowej Straży Pożarnej lub obiektem wskazanym przez tego komendanta. Obowiązek ten dotyczy budynków, obiektów budowlanych lub terenów objętych obligatoryjnym stosowaniem systemów sygnalizacji pożarowej, wyposażonych w urządzenia sygnalizacyjno-alarmowe, gdy w budynku, obiekcie budowlanym lub na terenie nie działa jego własna jednostka ratownicza.*



Rys. 1. Schemat systemu transmisji alarmów pożarowych



Dobrowolne podłączenie obiektu do komendy PSP

Ustawodawca nałożył obowiązek podłączenia do komend PSP określonych rodzajów budynków, ale przecież nie ogranicza to właścicieli innych budynków. Możliwe jest podłączenie do STAP budynków, dla których nie ma takiego obowiązku. Jeśli właściciel i administrator zauważą taką potrzebę, to wystarczy, by wykupili usługę transmisji alarmów pożarowych w jednej z firm, które taką usługę świadczą.

Ocena wyrobów, wymagane dokumenty i znakowanie

Systemy transmisji alarmów pożarowych – jako zestaw urządzeń UTAP + SOAP – są wymienione w załączniku do rozporządzenia Ministra Infrastruktury i Budownictwa z 17 listopada 2016 r. w sprawie sposobu deklarowania właściwości użytkowych wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania. Oznacza to, że wymagane jest dla nich znakowanie znakiem budowlanym oraz znakiem jednostki dopuszczającej. Ponieważ dla STAP nie istnieje Polska Norma wyrobu,

Wyrób specyfikacja techniczna	Wymagane dokumenty	Wymagane znakowanie
Zestaw wyrobów System transmisji alarmów pożarowych (STAP) Krajowa Ocena Techniczna	Krajowy certyfikat stałości właściwości użytkowych Krajowa deklaracja właściwości użyt- kowych Świadectwo dopuszczenia	
Element zestawu Urządzenie Transmisji Alarmów Pożarowych i Sygnałów Uszkodzenio- wych EN 54-21:2006	Certyfikat CPD lub Certyfikat CPR Deklaracja właści- wości użytkowych	

w procesie oceny właściwości użytkowych tego zestawu wyrobów wymagane jest opracowanie Krajowej Oceny Technicznej.

Natomiast dla UTAP, które stanowi element ww. zestawu wyrobów, norma została opracowana. Jest to PN-EN 54-21:2009 (EN54-21:2006; Systemy sygnalizacji pożarowej – Część 21: Urządzenia transmisji alarmów pożarowych i sygnałów uszkodzeniowych), która została zharmonizowana z rozporządzeniem 305/2011. Oznacza to zatem, że dla UTAPiSU wymagane jest uzyskanie oznakowania CE.

Nadajniki (UTAPiSU) powinny spełniać wymagania konstrukcyjne, funkcjonalne i środowiskowe określone w normie PN-EN 54-21:2009. Dla stacji odbiorczych alarmów takie wymagania określa Krajowa Ocena Techniczna dla Systemu Transmisji Alarmów Pożarowych.

Jednocześnie w trakcie badań laboratoryjnych, prowadzonych na potrzeby uzyskiwania certyfikatów urządzenia są poddawane różnego rodzaju badaniom środowiskowym, sprawdzającym m.in. odporność na niskie temperatury, wysoką wilgotność, uderzenia, wibracje sinusoidalne, zmiany napięcia zasilania, wyładowania elektrostatyczne itp.

Zasilanie i łączność – przynajmniej podwójne

Urządzenia służące do zabezpieczenia pożarowego budynków powinny być tak przygotowane, by na ich pracę nie wpływały ani brak zasilania, ani utrata łączności. Dlatego UTAPiSU powinny być wyposażone w rezerwowe źródło zasilania w postaci akumulatorów, które gwarantują pracę przez 72 godz., jeśli dojdzie do zaniku zasilania podstawowego. SOAP w przypadku zaniku zasilania podstawowego jest zasilana z agregatu prądotwórczego, w który są wyposażone komendy PSP.

Zdecydowanie więcej wymagań dotyczy transmisji. Do przesyłania alarmów pożarowych z UTAP do SOAP mogą być wykorzystywane:

- tory transmisji tworzone specjalnie na potrzeby przesyłania alarmów pożarowych (np. połączenie przewodem, własna sieć radiowa operatora),
- transmisja za pomocą sieci publicznych operatorów telekomunikacyjnych,
- łącza publicznych sieci telekomunikacyjnych (PSTN i ISDN).

Typ łącza transmisji alarmów	Wymagania związane z transmisją alarmów pożarowych i sygnałów uszkodzeniowych (zgodnie z PN-EN 50136-1-1)						
	Tor transmisji	Czas transmisji klasyfikacja D ^{c)}	Czas transmisji wartość maksymalna M ^{c)}	Czas monitorowania T ^{c)}	Dostępność klasyfikacja A ^{a)}	Zabezpieczenie przed podstawieniem klasyfikacja S	Bezpieczeństwo informacji klasyfikacja I
Typ1 ^{b)}	Specjalizowane tory transmisji	D4=10 s	M4=20s	T5=90s ^{d)}	A4 ^{a)}	S1	I0
Typ2 ^{b) e)}	Systemy łączności cyfrowej wyko- rzystujące publiczną sieć komutowaną	D4=10 s	M3=60s	T2=25 h (całe łącze) T5=90 s (dostęp do sieci)	A4 ^{a)}	S1	I0

a) ogólna dostępność systemu obejmująca wszystkie tory transmisji; b) dostępność wymagana przy uwzględnieniu redundancji torów transmisji; c) każdy z parametrów – D, M oraz T powinien być osiągnięty przynajmniej w jednym torze transmisji łącza typu 1 lub typu 2; d) dla systemów radiowych może być stosowany czas raportowania T3; e) w przypadku wykorzystania analogowej, publicznej, komutowanej sieci telefonicznej (PSTN) mogą być stosowane parametry D2 i M2.

Łącza transmisyjne powinny umożliwiać transmisję dwukierunkową równoczesną lub naprzemienną. W szczególności powinny umożliwiać wysłanie potwierdzenia odbioru każdej informacji alarmowej.

Jeżeli do przesyłania sygnałów alarmowych wykorzystywany jest tor radiowy, operator systemu monitoringu pożarowego powinien mieć odpowiednie pozwolenie radiowe na wyłączne korzystanie z niego. Nie dopuszcza się wykorzystywania częstotliwości, które nie wymagają posiadania pozwoleń radiowych. Jeśli tor radiowy jest podstawowym, to musi być on używany wyłącznie na potrzeby systemu transmisji alarmów pożarowych.

Do przesyłania alarmów pożarowych pomiędzy urządzeniem transmisji alarmów pożarowych a stacją odbiorczą alarmów pożarowych powinny być wykorzystywane co najmniej dwa łącza transmisji określone jako łącze podstawowe i łącze dodatkowe.

Należy stosować dwa fizycznie różne tory transmisji. Transmisja alarmów pożarowych w łączach podstawowym i dodatkowym powinna być inicjowana równocześnie i odbywać się niezależnie. **Czas transmisji (D)** i **związany z nim maksymalny czas transmisji (M)** – wymagania dotyczą pełnego czasu transmisji od przekazania sygnału alarmowego, przez system sygnalizacji pożarowej, do jego udostępnienia przez urządzenie powiadamiające lub przekazanie tego sygnału do systemu prezentacji informacji centrum odbiorczego alarmów pożarowych.

Czas monitorowania systemu transmisji (T) – wymagania dotyczą czasu przesyłania sygnału uszkodzeniowego od momentu wykrycia usterki w STAP przez UTAPiSU do odebrania wiadomości przez stację odbiorczą sygnałów uszkodzeniowych. Informacje o sprawności systemu oraz wykrytych uszkodzeniach powinny być zbierane i rejestrowane przez centrum monitorowania operatora systemu.

Dostępność (A4) – wymagania dotyczą dostępności systemu transmisji alarmów pożarowych i klasyfikacji systemów, określanej na podstawie dostępności łączy i torów transmisji, z których będzie korzystał. Dostępność A4 oznacza, że system powinien być dostępny przez 99,8% czasu i dotyczy wszystkich systemów transmisji, niezależnie od liczby podłączonych do systemu budynków. **Zabezpieczenie przed podstawieniem (S1)** – wymagania dotyczą zapewnienia środków umożliwiających wykrycie podmiiany nadajnika/odbiornika w nadzorowanym budynku – odbywa się

to poprzez nadawanie identyfikatorów lub adresów do wszystkich komunikatów transmitowanych w systemie.

Ochrona informacji (I0) – oznacza, że nie jest wymagana ochrona informacji, ale może być ona realizowana np. poprzez szyfrowanie, co zabezpiecza przed nieautoryzowanym odczytem lub modyfikacją informacji.

Podłączenie obiektu do monitoringu pożarowego oznacza, że straż pożarna otrzyma zgłoszenie nawet wtedy, gdy pożar będzie jeszcze niedostrzegalny dla osób przybywających w miejscu, w którym do niego doszło. I z tego powodu zarządcy nawet tych budynków, które nie podlegają ustawowemu obowiązkowi, powinni rozważyć ich podłączenie do monitoringu pożarowego. Jest ono realizowane po uzgodnieniach z właściwym miejscowo komendantem miejskim lub powiatowym Państwowej Straży Pożarnej. PSP nie pobiera opłat za przyłączenie obiektów do monitoringu pożarowego.

Należy jednak pamiętać, że wezwanie straży pożarnej na skutek fałszywych alarmów pożarowych może spowodować obciążenie operatora systemu monitoringu lub zarządcę obiektu kosztami nieuzasadnionej interwencji. Istotne jest zatem, aby system sygnalizacji pożarowej był konserwowany, a w przypadku prowadzenia w obiekcie jakichkolwiek prac, w których wyniku może dojść do wzbudzenia alarmu fałszywego (np. w wyniku zapylenia czujek podczas prac budowlanych), fakt prowadzenia takich prac należy zgłosić z wyprzedzeniem do SK PSP. Innym rozwiązaniem jest czasowe ostonięcie czujek lub zablokowanie na czas prac wybranej strefy systemu sygnalizacji pożarowej. ●

GRZEGORZ MROCZKO

Absolwent SGSP, oficer PSP, pracownik Zakładu Ocen Technicznych CNBOP-PIB, koordynator ds. testowania wyrobów innowacyjnych wg procedury KG PSP, przedstawiciel Polski w TC 72 Europejskiego KT (CEN), członek KT 264 i KT 323 PKN. Audytor jednostki certyfikującej w zakresie m.in. SSP, DSO, systemów wentylacji pożarowej, kabli i zespołów kablowych stosowanych w technicznych systemach zabezpieczeń ppoż.





Kompaktowy system sygnalizacji pożarowej POLON 3000

Bezpieczeństwo pożarowe obiektów to – zaraz po wymogu zapewnienia trwałości budynków – najważniejszy warunek, jaki muszą spełniać zarówno nowe, jak i już istniejące obiekty, niezależnie od swojej wielkości i przeznaczenia.

Mariusz Radoszewski

W wielu z budynkach instalacje ppoż. są obowiązkowe, co wynika wprost z przepisów prawa. W innych ich montaż jest dobrowolny, choć czasami dokonywany ze względu na warunki ubezpieczenia lub na wniosek przedstawicieli straży pożarnej.

W obiektach, które umownie zaliczamy do małych albo średnich, doskonałym rozwiązaniem jest najnowszy kompaktowy system sygnalizacji pożarowej, oparty na centrali serii POLON 3000.

Centrala POLON 3000 jest elementem kompaktowego adresowalnego systemu sygnalizacji pożarowej, w którego skład wchodzi również cała gama elementów liniowych opracowanych na potrzeby systemu.

System ten, zastępujący na wielu rynkach (polskim i zagranicznych), urządzenia serii POLON 4000 (z jego mniejszymi wersjami centrali POLON 4100 oraz POLON 4200), wyznacza standard w zakresie niewielkich systemów sygnalizacji pożarowej.



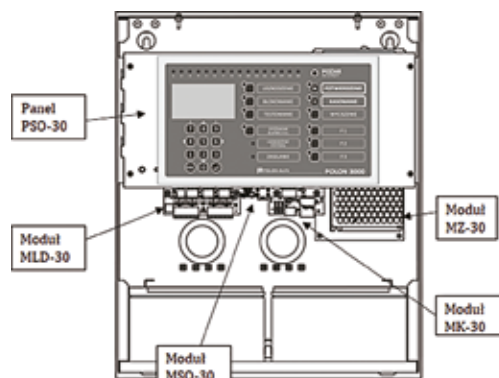
Centrala POLON 3000

POLON 3000 jest oferowany w trzech wariantach różniących się maksymalną liczbą elementów liniowych, które można do nich dołączyć:

1. POLON 3064 – maks. 64 elementów adresowalnych montowanych na 2 pętłach dozоровych (do 64 elementów na pojedynczej pętli),
2. POLON 3128 – maks. 128 elementów adresowalnych montowanych na 2 pętłach dozоровych (do 128 elementów na pojedynczej pętli),
3. POLON 3256 – maks. 256 elementów adresowalnych montowanych na 2 pętłach dozоровych (do 128 elementów na pojedynczej pętli).

Wymienione warianty (oraz elastyczność w zakresie doboru liczby elementów liniowych na pętłach centrali) umożliwiają stworzenie systemu zaprojektowanego najbardziej odpowiedniego dla chronionego obiektu.

Centrala POLON 3000 jest urządzeniem składającym się z modułów pełniących określone funkcje:



Moduł centralnego sterownika MSO-30

Główny moduł zarządzający centralą. Zawiera pamięć konfiguracji, pamięć operacyjną RAM i pamięć programu. Zapewnia wymianę danych między modułami, kontroluje sprawność wszystkich obwodów, analizuje i przetwarza odebrane sygnały oraz steruje wyjściami i interfejsem użytkownika.

Moduł linii dozоровych MLD-30

Interfejs komunikacyjny między centralą a elementami liniowymi. Linie dozоровe są zasilane napięciem 24 V. Moduł pozwala na podłączenie 2 linii (pętli) dozоровych. Obsługuje dołączone linie

dozоровe w układzie zarówno pętlowym – adresowalne linie dozоровe typu A, jak i promieniowym – adresowalne linie dozоровe typu B.

Moduł komunikacyjny MK-30

Moduł monitorowania stanu systemu poprzez Modbus TCP oraz Modbus RTU. Aby połączyć się z centralą, należy skonfigurować moduł MK-30 za pomocą aplikacji Polon Studio, korzystając z ww. protokołów.

Moduł zasilania MZ-30

Do działania centrali i jej podzespołów wymagane jest odpowiednie zasilanie. Odpowiada za to moduł zasilający MZ-30.

Nowe elementy liniowe serii 3000 współpracujące w systemie POLON 3000

Lp.	Typ elementu	Praca na linii dozоровej		Opis
		4000	6000	
1	DUO-3000	+	+	ostrzegacz pożarowy (czujka dualna dymu)
2	DUT-3000AD	+	+	ostrzegacz pożarowy z sygnalizatorem akustycznym (czujka optyczno-temperaturowa)
3	DOT-3000	+	+	ostrzegacz pożarowy (czujka optyczno-temperaturowa)
4	DOP-3000	+	+	ostrzegacz pożarowy (liniowa czujka dymu)
5	ROP-3000M / 3000MH			ręczny ostrzegacz pożarowy
6	EKS-3021 / 3022 / 3222P	-	+	element kontrolno-sterujący
7	SAW-3001	+	+	sygnalizator akustyczny (tonowy)
8	SAW-3006	+	+	sygnalizator akustyczno-głosowy
9	SAB-3001	+	+	sygnalizator optyczny, tonowy
10	SAB-3006	+	+	sygnalizator optyczny, tonowo-głosowy
11	Urządzenia zawierające moduł MKA	+	+	MKA – moduł komunikacji adresowalnej, umożliwiający adresowanie w pętli urządzeń typu UCS 6000 czy IGNI5 2500

Elementy liniowe współpracujące z centralami POLON 3000

Na dowolnej linii dozоровej centrali POLON 3000 mogą pracować adresowalne elementy liniowe szeregu 3000, opracowane specjalnie dla tego systemu. Linie dozоровe centrali zostały przystosowane również do obsługi elementów liniowych szeregów 4000 i 6000 produkcji POLON-ALFA, do tej pory używanych z adresowalnymi centralami serii POLON 4000 oraz POLON 6000. Umożliwia to stosowanie bardzo szerokiej gamy urządzeń (w zakresie wykrywania i sygnalizowania pożaru oraz sterowania urządzeniami zabezpieczającymi) i sprawia, że mogą być realizowane nawet skomplikowane scenariusze pożarowe.

Mikroprocesorowe czujki pożarowe

Z centralami systemu POLON 3000 mogą pracować czujki szeregu 3000 (wymienione w tabeli), czujki szeregu 4000 (optyczne dymu DOR, optyczno-plotmieniowe DPR i radiowe czujki dymu DUR-4047) i szeregu 6000 (DUO – z podwójnym układem detekcji dymu IR i UV, wielosensorowe czujki dymu i ciepła DOT – z podwójnym układem detekcji dymu IR i UV oraz podwójnym układem detekcji ciepła oraz adresowalne czujki liniowe dymu DOP-6000, a także nowo opracowane czujki DOT-6046 i DOT-6043).

Ręczne ostrzegacze pożarowe ROP-3000/3000H oraz ROP-4001M/4001MH

Informacje przekazywane do centrali przez ręczne ostrzegacze pożarowe uważane są za priorytetowe, zakładają bowiem świadome użycie ich przez człowieka. Ostrzegacze w wersji szczelnej, oznaczone jako ROP-3000MH i ROP-4001MH, mogą być instalowane na zewnątrz obiektu.

Adresowalne sygnalizatory serii SAW i SAB serii 3000 i serii 6000

Adresowalne sygnalizatory akustyczne SAW-300x/600x są przeznaczone do lokalnego akustycznego sygnalizowania pożaru w sposób tonowy (SAW-3001/6001) lub tonowo-głosowy (SAW-3006/6006). Do poprawnej pracy (oprócz zasilania z linii dozоровej) wymagają również podłączenia zewnętrznego zasilacza ppoż.

Dostępne są także adresowalne sygnalizatory optyczno-akustyczne SAB-300x/600x, które są przeznaczone do sygnalizowania o wystąpieniu pożaru za pomocą błysku i tonowo (SAB-3001/ 6001) lub tonowo-głosowo (SAB-3006/6006).

Sygnalizatory występują w dwóch kolorach obudowy i światła błysku ostrzegawczego: czerwonym – z oznaczeniem literowym RR i białym – z oznaczeniem WW.

Adresowalne elementy kontrolno-sterujące

Dla adresowanych programowo elementów kontrolno-sterujących istnieje możliwość uruchamiania dodatkowych urządzeń przeciwpożarowych lub sygnalizacyjnych w instalacji, a także kontrolowania urządzeń do niej dołączonych.

Elementy, oprócz przekątnikowych wyjść sterujących, mają wejścia kontrolne do nadzorowania sterowanych urządzeń lub do niezależnego wykorzystania (lub „tylko wyjścia sterujące” albo „tylko wejścia kontrolne”).

Programowanie central POLON 3000

Do zaprogramowania (konfigurowania ustawień) central POLON 3000 służy oprogramowanie POLON Studio dostępne dla instalatorów, którzy wcześniej odbyli odpowiednie szkolenie.

W aplikacji jest możliwe, w sposób graficzny i opisowy, zadeklarowanie wariantu centrali podlegającej konfiguracji oraz precyzyjne ustawienie wszystkich parametrów i funkcji samej centrali oraz jej elementów liniowych. W efekcie tworzony jest plik konfiguracji, który należy przesać do centrali (z poziomu komputera, łącąc się do modułu głównego centrali kablem USB typu A-B).



Przykładowe okna konfiguracji programu POLON Studio

Kompaktowy system sygnalizacji pożarowej POLON 3000 to kolejny krok POLON-ALFA w celu zaoferowania klientom w Polsce i za granicą nowoczesnego, bardzo funkcjonalnego i elastycznego w stosowaniu rozwiązania w zakresie zabezpieczenia przed pożarami w obiektach małej i średniej wielkości. Nowy wzorec bezpieczeństwa? Z pewnością tak. ●

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
www.polon-alfa.pl



Higiena bezpiecznej pracy zdalnej

Bez wątpienia pandemia COVID-19 przyspieszyła to, co było nieuchronne, czyli upowszechnienie pracy zdalnej. Ten sposób wykonywania obowiązków nie jest efektem czy dziełem tylko pandemii, był oczywiście stosowany już wcześniej. Niemniej jednak na dużo mniejszą skalę, ograniczoną do wybranych zawodów.

Tomasz Dacka

Obostrzenia epidemiczne spowodowały, że wiele przedsiębiorstw z dnia na dzień stanęło przed olbrzymim wyzwaniem, jakim była konieczność wprowadzenia pracy zdalnej. Wyzwania te można podzielić na dwa rodzaje. Pierwszym są wyzwania techniczne związane z tym, że praca zdalna wymaga odpowiedniej infrastruktury IT nie tylko sprzętowej, ale także programowej, służącej zapewnieniu m.in. cyberbezpieczeństwa (np. VPN, VDI, zarządzanie certyfikatami). Nie wszystkie firmy były na to przygotowane.

Drugi rodzaj to wyzwania, który można nazwać mentalnym. Kadra menedżerska nagle straciła podwładnych z oczu. Praktycznie dosłownie. Jednocześnie pracownicy musieli zmienić swoje przyzwyczajenia i podejście do pracy. W wielu firmach zmodyfikowano sposób rozliczania pracy, a spotkania wideokonferencje zastąpiły spotkania w salach konferencyjnych.

Wspólny mianownik

Oba wyzwania miały wspólny mianownik: konieczność zadbania o przygotowanie takiego cyfrowego środowiska pracy, które zapewni użytkownikom optymalne warunki pracy, a jednocześnie będzie chronić dane gromadzone i przechowywane przez firmy.

Wprowadzenie takiego środowiska wymagało oczywiście czasu i odpowiednich zasobów. Nie stało się to z dnia na dzień, z czego skrupulatnie korzystali tzw. źli aktorzy, czego dowodem była gwałtownie rosnąca podczas pandemii liczba ataków hakerskich. Patrząc z perspektywy czasu, może się wydawać, że jeśli chodzi o cyfrowe bezpieczeństwo IT w kontekście pracy zdalnej, to najgorsze jest już za nami. Jednak nie powinniśmy spoczywać na laurach, do czego firmy i użytkownicy mają tendencję. Miałem ostatnio okazję zapoznać się z wynikami audytów przeprowadzonych w dużych przedsiębiorstwach, na potrzeby których zastosowano atak phishingowy. Rezultaty tych sfingowanych ataków nie napawają optymizmem. Warto zatem przypomnieć

najważniejsze aspekty bezpiecznego funkcjonowania w zdalnym cyfrowym środowisku pracy.

Świadomość pracowników ma kluczowe znaczenie

Zdecydowanie najważniejszy, kluczowy aspekt całości układanki. Żadne kampanie, najznamienitsze systemy defensywne oparte na wielowarstwowych modelach ochrony nie pomogą, jeśli użytkownik nie będzie w sposób odpowiedzialny korzystał z powierzonych zasobów. Możemy zadać sobie pytanie, kiedy ostatnio czytaliśmy politykę bezpieczeństwa naszej organizacji. Zapewne znajdziemy tam kilka załączników dotyczących bezpieczeństwa fizycznego i teletechnicznego. Te dokumenty nie powstały na potrzeby audytów, lecz by nam, użytkownikom, na co dzień pomagać w sposób bezpieczny (a przynajmniej zgodny z przyjętymi wytycznymi) świadczyć swoją pracę. Dopóki przestrzegamy zapisów, dopóty jesteśmy chronieni i zgodni, a odpowiedzialność jest przenoszona na komórki odpowiedzialne za kwestie techniczne.

Rutyna bywa niebezpieczna

Skoro do tej pory nic się nie stało, oznacza to, że robię wszystko dobrze. Nawet nie wiem, kiedy machinalnie zaczynam wykonywać czynności. Kolejne cykliczne szkolenia odbywam na zasadzie odhaczenia obecności. Sami tworzymy tym samym żyzne podłoże dla nieuprawnionych ingerencji.

Aktualizacja wiedzy

Informacje o zagrożeniach i sposobach przeciwdziałania atakom powinny być aktualizowane równie często jak nasz system antywirusowy, czyli po pierwsze często. Po drugie aktualizacja powinna być częścią większego ekosystemu, tworząc holistyczny obrazek zapewnienia bezpieczeństwa naszym aktywom, a do nich należą nie tylko narzędzia pracy, ale także informacje przetwarzane za ich pomocą. Skąd zatem czerpać wiedzę? Jesteśmy nią obecnie wręcz



» Żadne kampanie, najznamienitsze systemy defensywne oparte na wielowarstwowych modelach ochrony nie pomogą, jeśli użytkownik nie będzie w sposób odpowiedzialny korzystał z powierzonych zasobów. «



zalewani, czego dobitnym przykładem jest również ten artykuł. Najlepiej korzystać ze sprawdzonych oficjalnych źródeł. W partykularnych organizacjach w sposób różny można podchodzić do kwestii bezpiecznej pracy, polecam zatem (jak zostało wspomniane już wcześniej) zacząć od wewnętrznych polityk, regulacji, wytycznych.

Informowanie o ataku

Firma każdej wielkości może paść ofiarą cyberataku. Nie ma znaczenia, czy to rodzinny zakład, czy korporacja międzynarodowa z ogromnym budżetem. Udany atak to najczęściej efekt ludzkiego błędu lub niedopatrzenia. Jeśli to nasz błąd, to nie wolno problemu ukrywać. Każdy taki incydent należy jak najszybciej zgłosić zgodnie z wewnętrznymi procedurami. Co jednak zrobić, jeśli nie wiadomo, czy faktycznie doszło do ataku. Droga jest dokładnie taka sama. Zgłaszamy i upewniamy się, że osoby odpowiedzialne za reagowanie na incydenty podejmą odpowiednie działania.

Dobre praktyki

Zacznijmy od tego, że sami powinniśmy dbać o powierzone nam narzędzia i dane. Firma przekazuje nam np. laptop, telefon, auto itp. Sprzęt może zostać skradziony lub uszkodzony. Warto zadbać, aby nie był nadto ekspozycyjny czy w przypadku osób pracujących mobilnie pozostawiany bez opieki, np. w aucie, kawiarni czy w pociągu. Rozsądne jest także ubezpieczenie firmowych urządzeń od kradzieży czy na wypadek uszkodzenia.

Obecnie większą wartość niż sam sprzęt mają przechowywane na nim dane. W jaki sposób zadbać, by np. w przypadku utraty laptopa firmowe dane nie trafiły w niepowołane ręce? Oto zestaw dobrych praktyk, które warto wdrożyć w organizacji, by uniknąć np. wycieku danych:

- **Szyfrowanie dysków** – osoba niepowołana, która wejdzie w posiadanie urządzenia, nie będzie w stanie dostać się do zawartości dysku. Jednym z popularnych rozwiązań do szyfrowania jest BitLocker – domyślnie instalowana w systemach Windows funkcja służąca do szyfrowania danych.
- **Praca przez VPN (Virtual Private Network)** to specjalna usługa, która umożliwia łączenie się z Internetem za pomocą szyfrowanego tunelu, który ukrywa i maskuje zarówno dane przesyłane przez sieć, jak i prawdziwy adres IP oraz lokalizację korzystającego z niej użytkownika. Za pomocą tej usługi użytkownik może łączyć się z firmowymi zasobami w sposób bezpieczny, cała transmisja jest bowiem szyfrowana. Dlatego do pracy zdalnej, szczególnie przy połączeniu z firmowymi serwerami, zaleca się stosowanie VPN.
- **Blokowanie stron internetowych** – wdrożone polityki bezpieczeństwa firmy mogą zawierać blokowanie niektórych stron, ponieważ wielu cyberprzestępców wykorzystuje ten wektor ataku.
- **Redundancja procesów** – mamy wdrożony proces zgłaszania incydentu. Możemy to zazwyczaj zrobić za pomocą portalu zgłoszeniowego lub przez telefon. Co natomiast w sytuacji, kiedy z pewnych względów nie mamy dostępu do komputera i telefonu służbowego (np. kradzież, brak zasięgu lub rozładowanie baterii). Warto we własnym zakresie zbudować dodatkowy kanał informowania, może to być zapisanie numeru do Service Desku/przełożonego na kartce/w prywatnym telefonie.
- **Stosowanie fizycznego filtru prywatyzującego na ekran** – niby drobiazg, a rzecz bardzo przydatna. Taki filtr, zdejmowany lub mocowany na stałe, w znacznym stopniu ograniczy kąt, pod jakim widoczny jest obraz na ekranie. Jeśli pracujemy w strefach ogólnodostępnych, zdecydowanie warto wyposażyć się właśnie w takie zabezpieczenie.

Bez wątpienia wypracowane dziś mechanizmy ochrony jutro mogą być niewystarczające ze względu na zagrożenia związane z nowymi technologiami lub lukami pojawiającymi się w już używanych. Modele pracy będą również ewoluować czy to za sprawą przepisów prawa, czy możliwości technicznych. Ostatnie lata udowodniły, że to, co niewykonalne do tej pory, może zostać wdrożone w szybkim tempie, i to bez uszczerbku dla jakości naszej pracy. Niezmienna pozostaje natomiast jednak kwestia: to my jesteśmy odpowiedzialni za to, jak wykorzystujemy i chronimy powierzone nam narzędzia i dane. •



Tomasz Dacka

Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

the future of PSIM is here.

psim.pl

integracja | korelacja | reakcja
stabilność | profesjonalizm | elastyczność

developed in Poland since 2011

WOJSKOWA AKADEMIA TECHNICZNA

Seminarium Branży Elektronicznych Systemów Bezpieczeństwa

Spotkanie firm z branży elektronicznych systemów bezpieczeństwa w ramach seminarium organizowanego przez Instytut Systemów Elektronicznych Wydziału Elektroniki Wojskowej Akademii Technicznej stało się coroczną tradycją. W tym roku po raz pierwszy trwało dwa dni.

Spośród ponad 20 partnerów z branży, z którymi Wydział Elektroniki WAT współpracuje od wielu lat, w tegorocznym wydarzeniu aktywnie uczestniczyły: AAT Systemy Bezpieczeństwa, Assa Abloy, Bosch Security and Safety Systems, CBC Poland, Hikvision, ICS Polska, ID Electronics, Janex International, Polon-Alfa, Polska Izba Systemów Alarmowych (PISA), Pulsar, Roger, Satel, Schrack Seconet oraz Szkoła Główna Służby Pożarniczej (SGSP). Magazyn „a&s Polska” był jednym z patronów medialnych wydarzenia.

Tematem przewodnim tegorocznej edycji seminarium były najnowsze rozwiązania produktowe oraz ich integracja z systemami kontroli dostępu. Wystąpienia uczestników w głównej mierze koncentrowały się na prezentacji najnowszych rozwiązań i wskazywaniu możliwości ich integracji z innymi systemami bezpieczeństwa. Zastosowanie sztucznej inteligencji do przetwarzania obrazu z monitoringu wizyjnego i wykorzystanie uzyskiwanych w ten sposób informacji jako czynnik integrujący różne systemy bezpieczeństwa przewijało się w wielu prezentacjach.

Jednym z wydarzeń seminarium jest konkurs o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa skierowany do studentów specjalności: Inżynieria Systemów Bezpieczeństwa na kierunku Elektronika i Telekomunikacja. Zwycięzcą i zdobywcą statuetki został inż. Piotr Wiski, student studiów II stopnia na kierunku elektronika i telekomunikacja. Tytuł pierwszego i drugiego wice-mistrza wywalczyli inż. Adrian Gronowski i Filip Zalewski. Kolejnych siedmiu laureatów, którzy uzyskali największą liczbę punktów, otrzymało wyróżnienia. ●



AXIS COMMUNICATIONS

Kamera termowizyjna do zdalnego monitorowania temperatur

Axis Communications wprowadza na rynek nową kamerę termowizyjną – AXIS Q2101-TE, która może mierzyć temperaturę w wyjątkowo szerokim zakresie od -40 do aż 350°C. W sytuacji przekroczenia ustalonego progu, gdy temperatura wzrośnie lub spadnie zbyt szybko, kamera uruchamia powiadomienie. Pozwala to na uniknięcie niepożądanych przestoju w produkcji spowodowanych przegrzewaniem się sprzętu, jak również konserwację predykcyjną.



Urządzenie wyposażono w najnowszy system-on-chip – ARTPEC 8, którego zadaniem jest obsługa funkcji analitycznych. Dzięki wczesnej detekcji ognia odpowiednie jednostki zostaną błyskawicznie powiadomione o wszelkich sygnałach mogących oznaczać wystąpienie pożaru. Funkcje analityczne umożliwiają również inteligentne filtrowanie sygnałów w celu zmniejszenia liczby fałszywych alarmów, ignorując np. powiadomienie o ciepłej rurze wydechowej przejeżdżających pojazdów roboczych. Kamera jest także wyposażona w elektroniczną stabilizację obrazu (EIS), która zmienia największe wibracje w stabilny obraz.

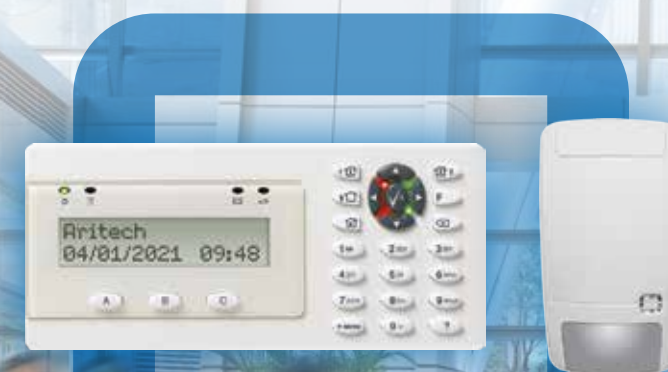
Odpowiednio zamontowana może monitorować teren w zakresie do 360°. Kontrola temperatury może dotyczyć aż 256 wcześniej zdefiniowanych obszarów, każdy zbudowany z 10 unikatowych wielokątnych obszarów zaznaczonych w systemie. Miejscowe wykrywanie temperatury umożliwia pobieranie danych z konkretnego miejsca, co pozwala zbierać informacje do badań, statystyk lub innych celów. Urządzenie ma także wbudowane dodatki z zakresu cyberbezpieczeństwa, które uszczelniają ochronę, utrudniając nieautoryzowany dostęp. Axis Edge Vault broni system identyfikacji, jednocześnie upraszczając autoryzację produktów Axis w sieci.

Kamerę wyróżniają duża wytrzymałość i odporność na uderzenia, co gwarantuje obudowa o klasie IK10. Jest przystosowana do pracy na zewnątrz, sprawdzi się w ochronie obwodowej oraz wykrywaniu i rejestracji zdarzeń z dużej odległości. Ochronę przed korozją potwierdza stopień ochrony obudowy IP66/67 i NEMA 4X. ●

 **ARITECH**

Advisor Advanced

Przeniesz cyberbezpieczeństwo na wyższy poziom



REKLAMA



Innowacyjny



Skuteczny



Idealny dla klienta

Aritech jest globalną marką firmy Carrier reprezentującą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferujemy zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, wideo i wykrywania pożaru. Aritech cieszy się zaufaniem klientów od ponad 40 lat.

Odwiedź: pl.firesecurityproducts.com



ZKTECO

MST150 PRO – bramka zintegrowana z wykrywaczem metali

Firma ZKTeco opracowała innowacyjne rozwiązanie zwiększające skuteczność kontroli bezpieczeństwa w postaci bramki sensorycznej uchylniej, zintegrowanej z precyzyjnym wykrywaczem metali.

Łącząc proces inspekcji i kontroli dostępu w bramce udało się zautomatyzować te procesy oraz wprowadzić oszczędności zarówno sprzętowe, jak i osobowe. Dzięki temu rozwiązaniu znacznie zwiększono również wydajność kontroli w miejscach wymagających wyższego poziomu zabezpieczeń, przy jednocześnie wysokim przepływie osób.

Urządzenie ma zastosowanie w takich obiektach, jak sądy, banki, obiekty wojskowe i infrastruktury krytycznej, budynki rządowe. Sprawdza się w miejscach o dużym przepływie osób, np. zakładach produkcyjnych, szkołach, stacjach kolejowych, w muzeach, wystawach czy innych budynkach użyteczności publicznej.

Cechy urządzenia:

- zintegrowana konstrukcja i łatwość rozbudowy o inne elementy kontroli dostępu,
- elegancka otwarta konstrukcja wytrzymała na uderzenia mechaniczne,



- prosty montaż i konfiguracja zestawu, obudowa łatwa w utrzymaniu,
- 15 stref wykrywania metali, każda o niezależnie regulowanym poziomie czułości,
- wbudowany wyświetlacz LED ułatwiający konfigurację,
- wskaźnik przejścia oraz wbudowany alarm dźwiękowy i wizualny,
- precyzyjny serwomotor o wysokiej wydajności przekładni, blokada nieautoryzowanego przejścia, w tym przejścia 2 osób jednocześnie, forsowania bramki, przejścia w kierunku przeciwnym. ●



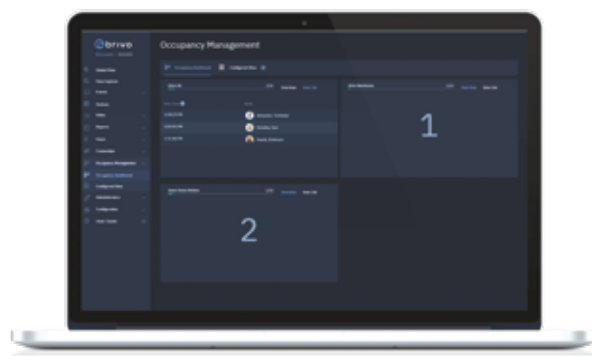
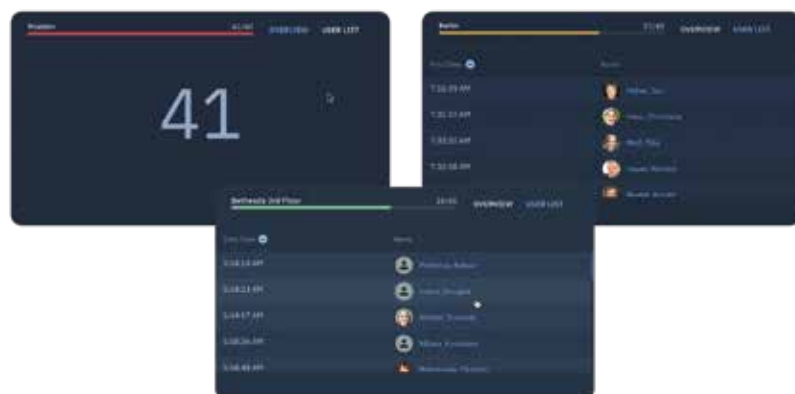
SMART-I

Brivo – zarządzanie liczbą pracowników w obiekcie

Zarządzanie obłożeniem to funkcja udostępniona w chmurowej platformie Brivo Access. Umożliwia kierownikom ds. bezpieczeństwa ustalanie obecności pracowników w poszczególnych lokalizacjach, z uwzględnieniem wymagań korporacyjnych lub lokalowych.

W panelu nawigacyjnym prezentowane są liczby osób przebywających w obiekcie. Z tego miejsca administratorzy mogą przejrzeć listę obecnych osób. Funkcja ta pozwala na szybkie podejmowanie decyzji dotyczących dostępu do obiektu w sytuacji, gdy frekwencja przekracza założony limit.

Zarządzanie limitami liczby pracowników jest kluczowe, by proces powrotu do biur po czasach pracy zdalnej lub hybrydowej odbywał się płynnie i zakończył się sukcesem. W związku z tym funkcja monitorowania obecności jest cennym rozszerzeniem funkcji bezpieczeństwa obiektu. Funkcje te, w połączeniu z możliwością raportowania wizyt użytkowników oraz gości, pozwalają na łatwiejsze planowanie kosztów eksploatacyjnych przestrzeni firmowych. Platforma Brivo umożliwia prosty eksport tych danych za pomocą wbudowanego modułu Data Explorer. Natomiast integratorzy rozwiązań wspierających pracę hybrydową mogą korzystać z otwartego API Brivo. ●



Sensoryczne bramki kontroli dostępu serii **SBTL6000** i **FBL6000 Pro**

Innowacyjne systemy bezkontaktowej kontroli przejść
zaprojektowane z myślą o płynnym działaniu

ZKTeco




Monitoring
pojedynczego
przejścia w obu
kierunkach


Przeciwdziałanie
przejściu kilku
osób na raz


Alarmowe
odblokowywanie
przejścia


Zabezpieczenie
antywywypadkowe


Ochrona przed
ściśnięciem osoby
przechodzącej


Możliwość
przejazdu wózka
inwalidzkiego

Doskonała współpraca z systemami kontroli dostępu
i rejestracji czasu pracy firmy ZKTeco

ZKTeco Europe
www.zkteco.eu
marketing@zkteco.eu



AAT SYSTEMY BEZPIECZEŃSTWA

Nowa efektywniejsza platforma zamówień AAT

Firma AAT Systemy Bezpieczeństwa od wielu lat dostarcza klientom kompleksowych rozwiązań z dziedziny elektronicznych systemów zabezpieczenia mienia. Współpracę z nabywcami ułatwia opracowana przez AAT platforma zamówień, która jest sukcesywnie rozwijana.

Obecnie dzięki nowoczesnym rozwiązaniom klienci mają dostęp do szeregu nowych funkcji, w tym m.in.:

- informacji o limicie kredytowym: przyznanym, wykorzystanym oraz przeterminowanych płatnościach,
- wysokości rabatów przeznaczonych specjalnie dla klienta,
- promocji,
- podglądu zamówień oraz statusu ich realizacji (również dla zamówień złożonych poza platformą),
- historii faktur z ostatnich 3 miesięcy,
- tworzenia n-koszyków, dzięki którym kompletując zamówienie, można dodawać towary do wielu różnych koszyków, a także wskazać do każdego zamówienia inny adres wysyłkowy,
- powiadomień e-mail o statusie zamówienia,
- zaawansowanego filtrowania produktów z uwzględnieniem wielu parametrów,



- pełen wachlarz informacji marketingowo-technicznych zintegrowany ze stroną AAT.

Platforma zamówień AAT, oprócz produktów marek własnych NOVUS, KADE, ZEUS, EVIX oferuje w jednym miejscu wygodny dostęp do produktów pozostałych producentów elektronicznych systemów zabezpieczeń. Dzięki temu można łatwo, wygodnie i efektywnie wybierać spośród szerokiego wachlarza wysokiej jakości artykułów, bez konieczności korzystania z wielu różnych źródeł.

Platforma zamówień AAT to możliwość składania zamówień o każdej porze dnia i nocy. Dodatkowymi atutami są również przejrzystość i nowoczesny design. Dzięki intuicyjnemu menu można łatwo znaleźć potrzebne urządzenia i w bezproblemowy sposób zbudować ofertę. ●



ROGER

Nowa wersja oprogramowania VISO do systemu kontroli dostępu RACS 5

Aplikacja VISO jest przeznaczona do zarządzania systemem kontroli dostępu RACS 5. Jej nowa wersja – v2.0.6 – wprowadza wiele udoskonaleń, wśród których do najważniejszych należą integrację z systemem ppoż. Cerberus (Siemens) oraz obsługa kolejnych rejestratorów i kamer (Hanwha Vision, BCS Point).



Nowe funkcje są uzupełnieniem dostępnych integracji systemu kontroli dostępu RACS 5 i w połączeniu z nimi tworzą rozwiązanie dla dużych instalacji, w których wymagane jest centralne zarządzanie systemem bezpieczeństwa z poziomu jednej platformy oprogramowania, którą w przypadku RACS 5 jest VISO SMS.

Do oprogramowania dodano wiele funkcji, wśród których należy wymienić możliwość obsługi kamer PTZ oraz definiowanie i realizowanie scenariuszy bezpieczeństwa w ramach VISO SMS. Scenariusze bezpieczeństwa pozwalają na tworzenie predefiniowanych procedur działania obsługi obiektu w razie wystąpienia sytuacji awaryjnych, szczególnie w sytuacji zagrożenia życia lub mienia. Możliwość sterowania kamerami PTZ, która jest rozwinięciem już istniejącej funkcjonalności oprogramowania VISO w zakresie telewizji przemysłowej, istotnie ulepsza i rozszerza możliwości weryfikacji zagrożeń oraz koordynowania działań zapobiegawczych.

Wśród nowości warto wymienić: możliwość mapowania pól danych w ramach integracji z usługami katalogowymi (Active Directory), aktualizację oprogramowania wielu kontrolerów MC16 jednocześnie oraz generowanie, eksport i wydruk identyfikatorów w formie kodu QR. Identyfikacja za pomocą kodu QR wydrukowanego lub wyświetlonego na ekranie telefonu pozwala ograniczyć wydatki na karty RFID, natomiast zastosowanie integracji z usługami katalogowymi umożliwia przeniesienie zarządzania użytkownikami do centralnego systemu, którym w tym przypadku jest usługa Active Directory. ●

Hanwha Vision

TNO-7180RLP – szybkoobrotowa kamera z funkcją rozpoznawania typu, marki, modelu i koloru pojazdu

Hanwha Vision, globalny dostawca rozwiązań wizyjnych, wprowadził na rynek szybkoobrotową kamerę ANPR TNO-7180RLP z technologią Global Shutter i rozdzielczości 3 Mpix umożliwiającą rozpoznawanie tablic rejestracyjnych pojazdów poruszających się z prędkością do 200 km/h na dwóch pasach ruchu.

Kamera jest wyposażona w nowe rozwiązanie ROAD AI firmy Hanwha, które wykorzystuje analizę wizyjną opartą na AI do identyfikacji typu, marki, modelu i koloru wykrytych pojazdów. Rozpoznaje 70 marek samochodowych, 600 modeli i 10 kolorów. Urządzenie jest wyposażone w globalną migawkę (Global Shutter), która zapewnia większą dokładność i wyrazistość przechwytywanych obrazów tablic rejestracyjnych, charakteryzuje się też wysoką częstotliwością odświeżania do 60 kl./s. Dostęp do nagrań można uzyskać za pośrednictwem Wisenet WAVE, Wisenet SSM oraz innych wiodących w branży programów do zarządzania materiałem wizyjnym, w tym Milestone i Genetec.

Kamera może rozpoznawać tablice rejestracyjne oraz marki/modely pojazdów z różnych regionów, w tym z Europy i Wielkiej

Brytanii, Kanady, USA, Australii i Nowej Zelandii, Wietnamu, Indonezji, Bliskiego Wschodu, Afryki Południowej i Rosji.

Dzięki kamerze TNO-7180RLP operatorzy stacji monitoringu zyskują lepszy wgląd w ruch uliczny, a planiści są w stanie uwzględnić wszelkie trendy przy modernizacji dróg lub stworzeniu nowych buspasów czy ścieżek rowerowych.

Aby uzyskać lepszy widok tablic rejestracyjnych aplikacja internetowa kamery TNO-7180RLP może zasugerować operatorom optymalny kąt pionowy, obrotu i poziomu. Kamera ma wbudowany adaptacyjny promiennik podczerwieni z trzema oddzielnymi promiennikami (krótki/szerokokątny, średni/średni i długi/tele), co pozwala na oświetlenie obszaru do 50 m. Urządzenie wyposażono również w obiektyw zmiennoogniskowy oraz 18-krotny zoom optyczny.

Obudowa TNO-7180RLP ma stopień ochrony IP66/IP6K9K, IK10+ i NEMA 4X, dzięki czemu kamera jest odporna na wodę, pył i akty wandalizmu. Może być zasilana przez PoE++, dostępna jest także opcja HPoE. Inną opcją jest zasilacz 12 VDC, który zapewnia większą odporność na nieoczekiwane wahania zasilania i elastyczność instalacji. ●



R E K L A M A

We are now
 Hanwha Vision

Advanced vision solutions.
 Combining video surveillance, AI & cloud
 to realise our customers' ambitions.

Formerly known as Hanwha Techwin

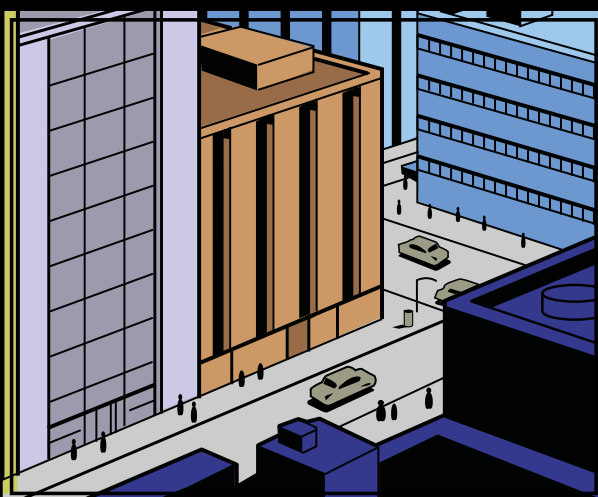
Tajemnica zaginionego segregatora

Robert Mietkowski pędził wąskimi osiedlowymi uliczkami na swoim dwukołowym rumaku. Do lśniącego nowością budynku Wydziału Inwestycji i Zamówień Publicznych Urzędu Miejskiego dopadł dobrze po 9.00, mruczając pod nosem: „Och, mili moi! Och, mili moi! Spóźnię się!”.

Chwila nerwowego poszukiwania karty wejściowej w niewielkim plecaku, trzy pary drzwi broniących dostępu do biura, krótkie przywitanie w recepcji i już prawie o czasie, czyli o 9.45 Robert Mietkowski, dla niepoznaki zwany Mietkiem, mógł zasiaść do żmudnej urzędniczej roboty.



Wydział Inwestycji i Zamówień Publicznych Urzędu Miejskiego, czule zwany Kamczatką, znajdował się w budynku zlokalizowanym na peryferiach miasta, więc wszyscy czuli się tu trochę jak na zestrzaniu. Miejsce zestrzania było jednak lubiane. Gmach był nowy, wejście skutecznie chronione przed namolnymi petentami, a open space sprzyjał integracji niewielkiego zespołu. Dobra kawa w pokoju socjalnym, zielen za oknem, polityka czystych biurek i wygodne szafy – czegoż chcieć więcej?



– Hej, nie widziałaś segregatora z przetargami? – Mietek pytająco spojrzął na Renatę, która ze skupieniem analizowała jakieś pradawne papierowe mapy. Koleżanka oderwała wzrok od ekranu i z nieprzytomną miną przecząco pokręciła głową. – Nieee, segregator? Ale jaki, taki żółty?



Szafy na klucz

Robert Mietkowski nie przepadał za polityką czystych biurek. Wolał własny artystyczny chaos. Rozumiał ją jednak doskonale. Urzędnicy zajmowali się często poufnymi sprawami, dokumenty nie mogły więc zalegać byle gdzie. Pod koniec dnia każdy segregator i teczka powinny trafić do zamykanej szafy. Praktyka ta była nieco uciążliwa, bo urząd było stać wyłącznie na tradycyjne szafy zamykane na klucz. Szybko więc się okazało, że teoria sobie, a życie sobie, o czym wkrótce boleśnie miał się przekonać nasz bohater.

Jak na spowiedzi

Specjalista okazał się specjalistką. Katarzyna Trzmieł jednak więcej miała z zajadłego szerszenia niż z puchatego trzmiela.

– **Panie Mieczysławie** – zaczęła oficjalnie, kiedy Robert Mietkowski wszedł do sali przesłuchań, czyli pokoju socjalnego, błyskawicznie zaadaptowanego na nieprzyjemną okoliczność zaginionych dokumentów.

– **Robercie** – szybko wtrąciła się recepcjonistka Kasia Miła, której zadaniem było notowanie i pilnowanie przestrzegania procedur.

– **Jak Robercie, skoro Mieczysławie?** – Trzmieł się zdziwiła.

– **Bo ja się nazywam Robert Mietkowski, dla znajomych Mietek** – wyjaśnił przycupnięty na krzeselku pechowy urzędnik.

– **Dobra, panie Mieczysławie, to znaczy Mietku, tego... Robercie** – Trzmieł trochę się pogubiła – **otóż obejrzałam nagrania monitoringu z ostatniego tygodnia i jedna rzecz mnie zastanawia, ale zapewne zaraz pan mi ją wyjaśni.**

– **Oczywiście** – zapewnił skwapliwie Mietek.

– **Co pan WYNIÓŚL wczoraj w tej reklamówce?!** – Trzmieł pacnęła w ekran laptopa, na którym wyraźnie było widać, że poza niewielkim plecakiem Mietek ma przy sobie plastikową torbę. – **Co pan wyniósł, czego rano pan nie wnosił?!**

Mietek poczuł, że zapada się w sobie. Palec Trzmieł cały czas oskarżycielsko pukał w ekran laptopa.

Długopis Kasi Miłej zawisł w powietrzu w oczekiwaniu na odpowiedź. Obecny na miejscu Tomasz Ojciec zamarł. Oczy całej trójki spoczęły na Mietku, który robił się coraz bardziej purpurowy, aż w końcu wykrztusił:

– **Piwo! Ale bezalkoholowe! Dokładnie puszkę po piwie bezalkoholowym, bo ja się muszę nawadaniać!**



– **Przecież wszystkie są żółte. Ten z szafy „Przetargi w toku”, który na końcu ma numer 102. Jest kolejny, czyli 103, a tego nie ma. Musi być w szafie, bo sam wczoraj tam go chowałem.** – Mietek przewrócił oczami.

Renata spojrzała jeszcze bardziej nieprzytomnym wzrokiem i wróciła do wpatrywania się w ekran. „Ech, z tej to pożytku nie będzie”, pomyślał Mietek i postanowił przepytac wszystkich pracowników. Pół godziny później poczuł, że wpada w lekką panikę. Po 40 minutach już na serio zaczął panikować. Bardzo WAŻNEGO segregatora nigdzie nie było. Jak kamień w wodę. Zbiorowa panika rozlała się na cały zespół. Wszyscy zaczęli sprawdzać, czy nikomu niczego nie brak. Nagle okazało się, że w szafie „Zlecenia” brak dwóch ważnych teczek. Nieprzytomna Renata nie może doliczyć się papierowych map geodezyjnych, a komuś zginął ulubiony kubeczek.

Kiedy nie dało się ukryć, że z biura zniknęły ważne dokumenty (nie zapominajmy też o ulubionym kubeczku), nadszedł czas na działanie. Kierownik wydziału Tomasz Ojciec powiadomił urząd o problemie zaginionych akt. Urząd, nie czekając, wysłał specjalistę ds. bezpieczeństwa fizycznego.



– Mietku, jak to tak? Piwo w pracy? – Kierownik nie krył zdumienia. – *Poza tym skoro bezalkoholowe, to czemu nie wniosłeś go oficjalnie? Przez recepcję?*

– *To skomplikowane* – wyszeptał Mietek.

– *Mniejsza z tym, czy piwo, czy kefir, czy wódka!* – ryknęła Trzmiel. – *Trzymajmy się faktów! Którędy pan je wniosł?!*

– *A to taka nasza mała tajemnica* – odpowiedział jeszcze ciszej Mietek.

– *Panie Mietku?! Jaka tajemnica? Niechże się pan nad nami zlituje, przecież oni nas tu wszystkich pozwalniają. Segregatora brak, mapy brak, wynieśli, zabrali, sam nie wiem co.* – Kierownik Tomasz nie krył zdenerwowania. – *Jak to się mogło stać, skoro tu teoretycznie mysz się nie prześlizgnie, a wszystko jest zamykane na klucz. Mietkowi nie pozostało nic innego, jak dokładnie opisać urzędniczy „przemytliczny szlak”.*



Opracowała Monika Mamakis na bazie scenariusza Jacka Grzechowiaka

Jak to się stało, że Robert Mietkowski wyniósł z firmy coś, czego do niej nie wniosł?

Odpowiedź na to pytanie poznali uczestnicy strategicznych warsztatów Forum Security prowadzonych przez Centrum Kompetencji a&s Polska. Warsztaty odbyły się 11 maja tego roku i wzięły w nich osoby zaproszone przez a&s Polska.

Centrum Kompetencji organizuje szkolenia i warsztaty dla osób odpowiedzialnych za bezpieczeństwo fizyczne, cyfrowe i zabezpieczenia techniczne.

Przekonaj się, co o warsztatach sądzą osoby, które wzięły w ich udział.

Monika Malczewska,
Urząd Miasta w Tomaszowie Mazowieckim

Już po raz kolejny uczestniczę w wydarzeniu organizowanym przez „a&s Polska” i zawsze wiedzę, którą zdobędę na nim wykorzystuję później w 100% w mojej pracy. Atutem tego typu szkoleń jest też oczywiście możliwość wymiany doświadczeń pomiędzy uczestnikami oraz specjalistami z różnych dziedzin. To szkolenie było wyjątkowe, bo oprócz dużej dawki wiedzy, zachęcało uczestników do brania czynnego udziału w ćwiczeniach. Bardzo dobrze słuchało się prowadzącego, był ekspresyjny i ciekawie opowiadał.



ppłk. Krzysztof Nawrocki,
Szpital Specjalistyczny im. Świętej Rodziny

Security Forum porównałbym do spektaklu w teatrze – mam tutaj na myśli przede wszystkim klimat i formę prowadzenia szkolenia, która przyciąga, zachęca i zaciekawia... tak jak teatr. Merytorycznie na najwyższym poziomie. Pan Jacek jest profesjonalistą, który ma ogromną wiedzę, a przy tym chce także słuchać i dyskutować, to niezwykle cenne. To była duża przyjemność być uczestnikiem tego wydarzenia.



Artur Hołubiczko, Komendant
Straży Miejskiej w Częstochowie
Dzisiejsze szkolenie było naprawdę na bardzo wysokim poziomie, a mam dużą skalę porównawczą, bo od 32 lat jeżdżę na przeróżne szkolenia w zakresie bezpieczeństwa i porządku publicznego. Świetny wykładowca, bardzo ciekawy tok wywodu, ładna prezentacja multimedialna prowadząca słuchacza krok po kroku do rozwiązania problemu. Chętnie piszę się na kolejne szkolenia.



check. create. manage.



BCS[®]

dla profesjonalistów

4^{city}

BCS-L-DMIP-4X5MWSIR3-V-A-AI2

4 wysokiej jakości kamery zamknięte w jednej obudowie. Każda z nich może być traktowana jako osobne urządzenie, przekazując oddzielne strumienie do rejestratora. Od strony instalacji traktujemy ją jako jedną kamerę, która pozwoli w łatwy sposób monitorować ciągi komunikacyjne w budynkach czy skrzyżowania ulic.



www.bcs.pl

www.facebook.com/bcspl

