

The logo for 'a&s' is displayed in a large, stylized font. The 'a' is blue, the ampersand is white, and the 's' is purple. The letters are set against a background of three vertical stripes: blue, black, and white.

POLSKA

**W CZASACH
PANDEMII**

→ 34

Bezpieczne szpitale

Branża security oferuje służbie zdrowia swoje rozwiązania: od kamer termowizyjnych i zintegrowania pomiaru temperatury ciała z systemami KD po systemy interkomowe i przyzywowe.

TEMAT
NUMERU

→ 46

Smart city
safe city

Technologie mobilne mogą w znacznym stopniu przyczynić się do zwiększenia bezpieczeństwa mieszkańców nie tylko w czasach pandemii.

PREMIERA

16

Bezpieczny biznes w TV

Pierwszy w polskiej telewizji program dotyczący tej tematyki. Autorska produkcja redakcji emitowana w telewizji BIZNES24 oraz online.

APLIKACJA
MOBILNA



a&s
POLSKA



15 zł
(w tym 8% VAT)

ISSN 2451-5175



052

POMIAR TEMPERATURY ROZWIĄZANIA TERMOGRAFICZNE

SAFER. FASTER. SMARTER



Wysoka wydajność

Tylko 1 SEKUNDA, by dokonać pomiaru temperatury

Bezpieczeństwo

Brak kontaktu – pomiar temperatury z odległości - bez kontaktu fizycznego

Dokładność

Dokładność pomiarowa: $\pm 0.3^{\circ}\text{C}$ z ciałem czarnym & $\pm 0.5^{\circ}\text{C}$ bez ciała czarnego



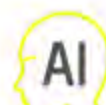
Brak kontaktu



Pomiar wielu
osób



Tylko 1 sekunda



Algorytm AI

REKOMENDOWANE PRODUKTY

- Zakres pomiarowy: $30-45^{\circ}\text{C}$
- Temperatura pracy: $10-35^{\circ}\text{C}$

DS-2TD2636B/P



- 384*288 rozdzielczość modułu termowizyjnego
- 15 mm ogniskowa obiektywu modułu termowizyjnego
- (Rekomendowana odległość pomiaru temperatury: 4.5-9 m)
- 6 mm ogniskowa modułu optycznego

DS-2TD2617B/PA



- 160*120 rozdzielczość modułu termowizyjnego
- 3/6 mm ogniskowa obiektywu modułu termowizyjnego
- (Rekomendowana odległość pomiaru temperatury: 0.8-1.5 m / 1.5-3.0 m)
- 4 / 6 mm ogniskowa modułu optycznego

DS-2TD1217B/PA



- 160*120 rozdzielczość modułu termowizyjnego
- 3/6 mm ogniskowa obiektywu modułu termowizyjnego
- (Rekomendowana odległość pomiaru temperatury: 0.8-1.5 m / 1.5-3.0 m)
- 4 / 6 mm ogniskowa modułu optycznego

DS-2TP21B-6AVF/W/P



- 160*120 rozdzielczość modułu termowizyjnego
- Max 8 MP rozdzielczość obrazu
- 6 mm ogniskowa obiektywu modułu termowizyjnego
- (Rekomendowana odległość pomiaru temperatury: 1.5-3.0 m)

Hikvision Poland
Hikvision Poland
ul. Żwirki i Wigury 16B
02-092 Warszawa
T. +48 22 4600150
info.pl@hikvision.com

Droży Czytelnicy

Pandemia COVID-19 wywołana koronawirusem SARS-CoV-2 wpłynęła na życie każdego z nas. Odczuwamy skutki izolacji, obostrzeń sanitarnych, pracy zdalnej. Sytuacja przewartościowała nasze życie zawodowe i prywatne. Zdominowała również naszą branżę. Bieżące wydanie zaczynamy od wskazówek dotyczących zapewnienia ciągłości działania miejsca szczególnego w całym systemie bezpieczeństwa – centrum monitorowania alarmów. Możliwość wprowadzenia kwarantanny wśród operatorów z powodu zarażenia się koronawirusem może bowiem wywołać poważny kryzys (s. 18).

W walce z pandemią sięgamy po różne środki. Z pomocą przychodzi także nowoczesna technologia. Dzięki niej branża security może wspomóc wiele sektorów gospodarki, m.in. służbę zdrowia. Bogatą ofertę rozwiązań dla placówek opieki medycznej, które stanęły przed koniecznością przystosowania swoich obiektów do nowych warunków funkcjonowania, przybliżamy w dziale bezpieczne szpitale (s. 34). Wyzwaniem jest zagwarantowanie odpowiedniej liczby miejsc dla chorych na COVID-19. I chociaż statystyki pokazują zwolnienie tempa pandemii, eksperci ostrzegają przed drugą falą zakażeń. O tym, jak zaadaptować budynki użyteczności publicznej na zastępcze miejsca szpitalne, piszemy na s. 42.

Jak w tej trudnej sytuacji radzą sobie miasta? Technologie smart city mogą w znacznym stopniu przyczynić się do poprawy bezpieczeństwa mieszkańców w czasie pandemii (s. 46). Trudno dzisiaj ocenić kierunki zmian i konkretne rozwiązania, niezbędne w tworzeniu nowej rzeczywistości po koronawirusie. Czy jednak wszyscy jednakowo rozumieją pojęcie bezpieczeństwa? Czy eksperci od bezpieczeństwa i mieszkańcy podobnie widzą pojawiające się problemy? (s. 74). Co zrobić, aby miasta stały się inteligentnie bezpieczne? (s. 52) Czy do problemu należy podchodzić całościowo, czy raczej skupić się na indywidualnym charakterze poszczególnych dzielnic? O tym, jak poziom bezpieczeństwa oceniają sami mieszkańcy, przeczytamy w analizie rankingu osiedli kilku polskich miast (s. 56). Pokazujemy także specyficzne doświadczenia światowych aglomeracji – o strategii odporności Bangkoku oraz bezpieczeństwie jego mieszkańców i turystów przeczytasz na s. 68. Aby idee smart city wcielić w życie, niezbędna jest odpowiednia infrastruktura, również telekomunikacyjna, która zapewni pewną i szybką wymianę danych. Pomocna będzie na pewno najnowsza technologia 5G. Czym jest i jakie ma zastosowania? Piszemy o tym na s. 22.

Wkraczamy w nowy etap naszej działalności – od czerwca zapraszamy do oglądania programu „Bezpieczny Biznes” (s. 16). Pod naszą redakcją w telewizji BIZNES24 powstaje pierwszy w Polsce program dotyczący bezpieczeństwa w prowadzeniu firmy. Pragniemy tą drogą przestrzec przed najczęściej popełnianymi błędami oraz promować najlepsze praktyki i uznanych specjalistów z branży. Mamy nadzieję, że program „Bezpieczny Biznes” stanie się cenionym, ciekawym źródłem informacji dla właścicieli, zarządców i kadry menedżerskiej polskich firm i instytucji. Chcemy w tych trudnych czasach dostarczać biznesowi rzetelnych porad i cennych informacji nt. zapewnienia bezpieczeństwa pracownikom i klientom, zarządzania kryzysowego oraz ciągłości działania firmy.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznick
Z-CIA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&s
POLSKA

www.aspolska.pl

Wydawca
A&S Polska Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznick

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

Redakcja
ul. A. Branickiego 15
Wilanów Office Park, bud. 1
02-972 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Kolegium redakcyjne
Norbert Bartkowiak
Sebastian Błażkiewicz
Marek Domański
Jacek Grzechowiak
Rafał Łupkowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Jacek Tyburek
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Prenumerata
www.aspolska.pl/prenumerata

Redakcja zastrzega sobie prawo skracania i adiacji zamówionych tekstów. Artykułów niezamówionych i niezatwierdzonych do druku nie zwracamy. Opinie autorów nie muszą być tożsame z poglądami redakcji. Za treść reklam redakcja nie odpowiada. Przedruki tekstów bez zgody redakcji są niedozwolone.

a&s Polska jest częścią grupy wydawniczej a&s International.

© Copyright by a&s Polska

A&S POLSKA
ZŁOTY PARTNER

AXIS
COMMUNICATIONS

BCS

HIKVISION

Linc
Polska Sp. z o.o.

SCHRACK
SECONET

TRUSTMAN

A&S POLSKA
SREBRNY
PARTNER

ahua
TECHNOLOGY

A&S POLSKA
WYDANIE
ONLINE

www.aspolska.pl/czasopismo

BCS[®]

dla profesjonalistów



Kamera termowizyjna dwuprzetwornikowa – kompletny zestaw do pomiaru temperatury ludzkiego ciała. Wysoce dokładny, szybki i bezkontaktowy pomiar temperatury wielu osób jednocześnie, automatyczna rejestracja i alert podwyższonej temperatury oraz braku maseczki ochronnej.



www.bcsctv.pl

BCS-TIP5240813-IR-TTW

kamera **mierzy**
i rejestruje
temperaturę
ciała

POLSKA
MARKA
BCS

8 Produkty numeru



16 Bezpieczny Biznes – premiera programu w BIZNES24

18 Plany awaryjne na wypadek wystąpienia koronawirusa w CMA
DANIEL KAMIŃSKI20 5G – Ultraszybka infostrada szerokopasmowa
JAN T. GRUSZNIC25 Sztuczna inteligencja w walce z pandemią
HIKVISION POLAND26 Autonomiczne układy kontroli dostępu i ich aktualizacja
PIOTR ŚWIDERSKI28 Systemy KD w biurach. O konieczności koordynacji prac projektowych
MICHAŁ ZALEWSKI32 SATEL KNX – automatyka budynkowa na najwyższym poziomie
SATEL

34 Bezpieczne szpitale z rozwiązaniami security. Zdalny pomiar temperatury

38 Bezpieczna komunikacja w sterylnych warunkach
C&C PARTNERS39 Systemy sygnalizacji pożarowej w służbie zdrowia w czasach COVID-19
JOHNSON CONTROLS INTERNATIONAL40 Wpływ pandemii koronawirusa na bezpieczeństwo w szpitalu
SCHRACK SECONET POLSKA42 Zastępcze miejsca szpitalne w budynkach użyteczności publicznej
ŁUKASZ STĘPIEŃ46 Smart city w dobie koronawirusa
JERZY MIKULIK49 Bezpieczne miasto według C&C Partners
C&C PARTNERS50 Smart city – więcej korzyści dzięki integracji zasobów
KONRAD BADOWSKI, AXIS COMMUNICATIONS52 W poszukiwaniu miasta inteligentnie bezpiecznego
BARTOSZ DOMINIAK55 Osiągnięcia Dallmeier w niemieckim sektorze Bezpieczne Miasto
DALLMEIER ELECTRONIC56 Miejski wymiar bezpieczeństwa. Krótka analiza Rankingu Dzielnic 2020 Otodom
RAFAŁ BATKOWSKI60 Na Kozłowiec – osiedle chronione jak miasto
SECURITAS POLSKA

62 CASE STUDY: Ciechanów – odpady pod e-kontrolą

64 CASE STUDY: Warszawa – parkowanie pod e-kontrolą

66 CASE STUDY: Gdynia – pierwsze miasto w Polsce z dostępem do sieci 5G

68 Przetwarzają odporni. Cz. 2. Strategia Bangkoku
JACEK TYBUREK

74 Głos branży

82 RODO a systemy kontroli dostępu. Cz. 1. Biometria w zatrudnieniu
PIOTR POWĄZKA86 Coś się kończy, coś się zaczyna. Finał sukcesji w Schrack Seconet Polska
SCHRACK SECONET POLSKA

88 Informacje firmowe





AXIS COMMUNICATIONS www.axis.com/pl

Pierwsza kamera nasobna od Axis

Axis Communications zaprezentowała pierwszą w swojej historii kamerę nasobną (tzw. *wearable*). AXIS W100 Body Worn Camera jest przeznaczona dla policji, straży miejskiej i firm ochroniarskich. Rozwiązanie oparte na otwartej architekturze systemowej obejmuje kamerę, stację dokującą i kontroler systemu. Możliwość integracji z dowolnym systemem zarządzania sprawą, że jest to najbardziej elastyczna kamera nasobna na świecie. Kamery nasobne mają wiele zalet: rejestrują materiał dowodowy, działają odstraszająco na przestępców, wspierają funkcjonariuszy i pracowników ochrony. Nasobna kamera

Axis może być stosowana z systemami VMS i EMS innych firm, może być też elementem kompleksowych rozwiązań, obejmujących oprogramowanie AXIS Camera Station i AXIS Case Insight.

Kamera generuje obraz o rozdzielczości do 1080p przy 30 kl./s oraz dźwięk (dwa mikrofony z funkcją tłumienia szumów). Funkcja WDR zapewnia wysoką jakość obrazu w trudnych warunkach oświetleniowych, a Axis Zipstream zmniejsza zapotrzebowanie na pamięć masową. Bateria umożliwia pracę do 12 godz., można ją doładowywać w samochodzie lub za pomocą powerbanku. Kontroler systemu umożliwia szybkie (100 Mb/s)

i niezawodne przesyłanie materiału wizyjnego z kamery. Dane są szyfrowane podczas transferu (AES256 i TLS) i przechowywania. W kamerę wbudowano także odbiornik GPS/GNSS do śledzenia lokalizacji, moduł Bluetooth Low Energy 4.1, moduł łączności Wi-Fi 802.11b/g/n, 6-osiowy żyroskop i akcelerometr.



BCS www.bcsctv.pl

Monitorowanie temperatury ciała

System dokładnego pomiaru temperatury ciała to dziś niezwykle przydatne narzędzie poprawiające poziom bezpieczeństwa w firmach. Może monitorować stan zdrowia pracowników przychodzących do pracy, klientów chcących wejść do sklepu czy osób w przychodni lekarskiej. Dzięki niezwykle dokładnemu pomiarowi temperatury, z marginesem błędów na poziomie 0,2°C, łatwo można wyłapać osoby z gorączką, stanowiące potencjalne zagrożenie dla osób znajdujących się w danym pomieszczeniu.

System składa się z dualnej kamery termowizyjnej BCS-TIP5240813-IR-TTW, z dwoma przetwornikami obrazu: termowizyjnym i z za-

kresu widzialnego o rozdzielczości 2 Mpix. Dzięki takiemu rozwiązaniu kamera przekazuje obraz zarówno termowizyjny, jak i wizyjny w kolorze. Ma też wbudowany głośnik i diodę LED do sygnalizowania zdarzeń alarmowych. Ważnym elementem systemu jest wzornik utrzymujący określoną wartość temperatury. Kamera, porównując tempe-



raturę osób, które się przed nią pojawiają, ze wzornikiem temperatury, mierzy ją z dokładnością do 0,2°C. Nie jest wrażliwa na zmiany temperatury otoczenia – nie wpływają one na dokładność pomiaru.

Ostatnim elementem systemu jest rejestrator BCS-IVS12808-Ai. Zapisuje informacje z kamery, a alarmy spowodowane przekroczeniem temperatury czy brakiem maseczki ochronnej może wyświetlić na podłączonym monitorze.

Montaż urządzeń ułatwiają dostarczane dwa stojaki, pomocne w zainstalowaniu kamery i wzornika na odpowiedniej wysokości i we właściwej odległości od siebie.

C&C PARTNERS www.ccpartners.pl

Nowa centrala alarmowa UNii – redundancja sprzętowa w systemach SSWN i KD



Rozwiązanie UNii ma budowę modułową. Dzięki jednej platformie sprzętowej system alarmowy można dostosować do aktualnych i przyszłych potrzeb klienta. Liczbę wejść w centrali można rozszerzyć z 32 do 128 lub 512.

Dodatkowe wejścia są aktywowane za pomocą licencji online, nie trzeba więc wymieniać płyty głównej centrali. Z centralą współpracują moduły rozszerzeń: dodatkowe wejścia, wyjścia OC i przekaźnikowe, ekspandery czytników KD, moduły do komunikacji urządzeń bezprzewodowych (Pyronix, PowerG, Elite), integracji automatyki KNX oraz dialery GPRS.

System jest dostępny w wersji z centralą redundantną gwarantującą 100 proc. dostępność przez 24 h/7. Za pomocą magistrali RS-485 centrale alarmowe

można łączyć w klastry, tworząc jeden system z maks. 4096 wejściami!

Manipulator jest kompaktowy, duże przyciski ułatwiają pracę, podświetlane klawisze nawigacyjne sprawdzają się idealnie w ciemnych pomieszczeniach. Można zaprogramować indywidualny język obsługi dla każdego użytkownika. W stanie bezczynności klawiatura jest w stanie uśpienia, uruchamia się automatycznie za pomocą czujnika ruchu.

Dzięki czytnikowi DESFire EV2 systemem można zarządzać za pomocą najbezpieczniejszej technologii zblizeniowej. Jest w pełni zgodny z normami serii EN50131 dla urządzeń stopnia 3 (Grade 3), ma świadectwo kwalifikacyjne TECHOM. UNii jest zintegrowane z rozwiązaniami BMS, SMS, VMS i PSIM.

Zintegrowany System Zarządzania Bezpieczeństwem

ICTProtegeGX®

Pomaga w zachowaniu obowiązkowego dystansu społecznego



Nowa wersja Protege 4.3.285 – już dostępna!

Zawiera szereg nowych funkcji i ulepszeń, m.in.:

- Integracja z Princeton Identity Biometrics - pozwala na zastosowanie skanerów tęczówki oka Princeton Identity zapewniając szybką i bezpieczną weryfikację tożsamości.
- Identyfikatory zgodności - umożliwiają kontrolę dostępu w oparciu o dodatkowe kryteria, poprawiając tym samym bezpieczeństwo i przestrzeganie procedur np. aktualne badania lekarskie, uprawnienia, dokumenty.

MIWI URMET Sp. z o.o.
ul. Pojezierska 90 A, 91-341 Łódź
Tel. +48 (42) 616 21 00
miwi@miwiurmet.pl
www.miwiurmet.pl

urmet
MIWI

**DAHUA TECHNOLOGY POLAND** www.dahuasecurity.com/pl

Rozwiązania w dobie walki z COVID-19 systemy zliczania ludzi

W obecnej sytuacji związanej z zagrożeniem Koronawirusem i kolejnymi restrykcjami wydawanymi przez rząd, zespół Dahua Technology intensywnie pracuje nad rozwiązaniami wspierającymi bezpieczeństwo w przestrzeni publicznej. Po sukcesie rozwiązań z zakresu pomiaru temperatury HBTM wprowadzamy na rynek rozwiązania PCFC, które mają na celu zliczanie osób wchodzących w określony obszar, kontrolowanie liczby osób w sklepie, aptece czy innych miejscach publicznych.

W naszym portfolio rozwiązań PCFC przygotowaliśmy trzy scenariusze:

- 1) zliczanie osób przekraczających linię lub statystyka liczby osób w obszarze dla małych rozwiązań, z jednym wejściem/wyjściem i sterowanie przełącznikiem;
- 2) informacje OSD – do tego rozwiązania potrzebna jest kamera AI PRO z serii IPC5xxx, do 4 wejść/wyjść, sumujemy statystyki przekroczenia linii z udziałem rejestratorów serii NVR5x-4ks2e;
- 3) system zliczania oparty na platformie DSS PRO do zliczania wielu wejść/wyjść w jednym lub wielu obszarach/sklepach itp. Dodatkową funkcją platformy DSS PRO jest możliwość integracji z rozwiązaniami Digital Signage w celu wyświetlania dynamicz-



nych komunikatów informujących o liczbie osób w obszarze, prowadzeniu nawigacji wejść/wyjść bez udziału osób czy głosowych komunikatów ostrzegających „Proszę czekać”, „Proszę wejść”.

Filmy pokazowe oraz informacje o webinarach online można znaleźć na naszym fanpage'u na Facebooku.

ELA-COMPIL www.ela.pl

GEMOS FM Expert

W jaki sposób opanować zmorę fałszywych alarmów? Odpowiedzią jest moduł analityczny FM Expert, stanowiący rozszerzenie funkcjonalności systemu GEMOS – uniwersalnej platformy integrującej i kontrolującej wszystkie systemy w obiekcie.

Moduł FM Expert analizuje dane, które GEMOS zbiera ze wszystkich zintegrowanych systemów, poddaje je filtracji, po czym w przejrzysty sposób prezentuje w formie wykresów graficznych. Pozwala szybko ocenić sytuację i zdecydować, która awaria wymaga reakcji w pierwszej kolejności. Prezentowane dane umożliwiają wypracowanie rozwiązań usuwających przyczyny, a nie tylko skutki awarii.



Moduł zapewnia płynne przejście od prezentacji statystyk, po wskazanie krytycznego punktu i jego lokalizacji na planie obiektu. Wspiera analizę incydentów, pozwala np. odtworzyć fragment

nagrania wideo z momentu wystąpienia alarmu, np. nadużycia w systemach KD czy nieuzasadnione wywołanie alarmu pożarowego.

FM Expert pozwala ocenić jakość wykonanych konserwacji na podstawie częstotliwości występujących awarii oraz analizować działania podejmowane przez personel ochrony. Wnioski z analizy pomogą wyeliminować niewłaściwe reakcje i tym samym dopracować procedury.

Jeżeli zajmujesz się Facility Managementem i masz problem z fałszywymi alarmami, ze sprawdzeniem, jak reagują operatorzy, z rozliczaniem prac konserwacyjnych, raportowaniem tego, co się dzieje w obiekcie, z oszacowaniem kosztów, których można uniknąć – GEMOS FM Expert jest rozwiązaniem dla Ciebie!

EUROALARM euroalarm.com.pl

SynovafoG na intruza i patogeny

Ze względu na zagrożenia, jakie niosą patogeny, firma Euroalarm wprowadziła do oferty generator mgły służący do odkażania pomieszczeń, opracowany na bazie sprawdzonych rozwiązań antykradzieżowych.

Obecnie generator mgły udostępnia obie funkcje: dezynfekcji oraz antykradzieżową. Urządzenie może (opcjonalnie) wykorzystywać dwie różne substancje chemiczne, mające działanie antybakteryjne i przeciwwirusowe. Oddziałuje także na wirusy z otoczką lipidową, w tym HIV i HBV.

W przeciwieństwie do ozonowania ta metoda jest bezpieczna dla ludzi w bezpośrednim kontakcie i może być wykorzystana do utworzenia zasłony dymnej w systemach antykradzieżowych. Jednocześnie można ją stosować cyklicznie do oczysz-

czania powietrza. Druga wersja zawiera podchloryn sodu zalecany przez WHO na COVID-19, a jej użycie odbywa się pod nieobecność ludzi. Mgła ustępuje samoistnie po trzech godzinach, nie pozostawiając śladu.

Wydajność generatora: 100 m³ pomieszczenia w czasie ok. 5 do 14 sekund, w zależności od modelu. Dostępne są urządzenia do zastosowania zarówno w małych, jak i dużych obiektach o kubaturze od 50 do 6000 m³. Filmy poglądowe można obejrzeć na YouTube Euroalarm (<https://www.youtube.com/watch?v=Xk1kAg82mIY>, <https://www.youtube.com/watch?v=zBSb2z03IHg>)

Generator mgły SynovafoG sprawdzi się w takich obiektach, jak hotele, kina, przedszkola, szkoły, biura, siłownie, szatnie, muzea, gabinety lekarskie, mieszkania.

ROZWIĄZANIE DO KONTROLOWANIA PRZEPŁYWU LUDZI

Precyzja, wydajność oraz funkcjonalność



Z myślą o obiektach handlowych, usługowych oraz infrastrukturze transportu publicznego, w czasach ryzyka zakażeniem wirusem COVID-19, Dahua Technology prezentuje rozwiązanie do zliczania ludzi oraz kontrolowania ich przepływu.

Ma ono zastosowanie wszędzie tam, gdzie zależy nam na wiedzy ile osób weszło do sklepu oraz ilu klientów nadal przebywa w środku. Możliwe jest również kontrolowanie ilości osób oczekujących w kolejce do punktu obsługi.

Rekomendowane produkty



IPC-HDBW5241R-ASE



Aplikacja DMSS



PFS3005-4ET-60



NVR5208-4KS2



DHL22-L200

CE FC CC UL R0012 ISO 9001:2000

**Dahua Technology Poland Sp. z o.o.**

ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com/ceen



PRODUKT NUMERU

GDE POLSKA www.gde.pl

Nowa jakość systemów wideodomofonowych COMMAX

COMMAX rozszerza gamę produktów wideodomofonowych o nowe modele rozdzielczości full HD. Monitor COMMAX CDV-70MF z panoramicznym 7" ekranem, oprócz obsługi standardowych kamer, wyświetla obraz z paneli wejściowych wyposażonych w optykę HD 1080p (2 Mpix), co przekłada się na 3-, 4-krotnie większą szczegółowość obrazu w porównaniu ze standardowymi kamerami analogowymi.

Zwiększenie jakości toru wideo nie wymaga dodatkowych zabiegów instalacyjnych – sys-

tem pracuje poprawnie na standardowym przebudowaniu. Monitor może też wyświetlać obrazy z dodatkowych kamer dozorowych pracujących również w rozdzielczości AHD 2 Mpix, a dzięki funkcji PIP wyświetla obrazy z panelu i dodatkowej kamery jednocześnie. Wbudowany moduł pamięci umożliwia zapisywanie zdjęć lub filmów podczas wywołania monitora oraz w przypadku wykrycia ruchu na obrazie z wybranej kamery. Obsługę ułatwia ekran dotykowy. Monitory są dostępne w dwóch wersjach kolorystycznych: klasycznej białopercowej oraz designerskiej ciemnoszarej z granatowym akcentem wokół ekranu.

Monitor obsługuje panele wejściowe COMMAX – zarówno analogowe, jak i szeroką gamę paneli z optyką HD 2 Mpix i 1,3 Mpix. Użytkownik może wybrać modele do montażu na wąskich słupkach (np. DRC-4CPHD) lub klasyczne (np. DRC-40YFD) oraz wyposażone w czytnik kart/breloków i/lub klawiaturę kodową, umożliwiające otwarcie furtki i bramy za pomocą kodu i/lub transpondera zbliżeniowego (np. DRC-40DKHD).



GDE POLSKA www.gde.pl

Monitoring 4K (8 Mpix) – kamera MAZi TWN-83MR



Firma MAZi rozszerza ofertę kamer analogowych HD-TVI o rozdzielczości 8 Mpix (3840 x 2160 pix) o tańsze modele serii N. Ich przykładem jest kamera kompaktowa (bullet) TWH-83MR. Dzięki 4x większej rozdzielczości niż typowe kamery 2 Mpix full HD zapew-

nia obraz o zdecydowanie większej szczegółowości i wyrazistości.

Kamerę wyposażono w obiektyw 3,3...12 mm moto-zoom z autofokusem do ustawienia pola widzenia kamery (automatycznie sama wyreguluje ostrość), a także w zdalne sterowanie funkcjami kamery z poziomu rejestratora. Dzięki temu za pomocą kabla koncentrycznego lub skrętki, po której przesyłany jest także obraz, można zdalnie sterować kamerami, tak jak w przypadku kamer IP. Zdalnie można regulować zoom, jasność, nasycenie kolorów i wiele innych parametrów (np. BLC, 3DNR, AWB, pracę moto-zoom). Kamery 8 Mpix wymagają kompatybilnych rejestratorów, np. HSVR-08HT1, HSVR-08HT,

HSVR-16HT. Zasięg połączenia zależy od okablowania, a w przypadku skrętki UTP od zastosowanych transceiverów. Typowo wynosi ok. 100m dla UTP i 200 m dla kabla koncentrycznego klasy RG59. Stosując kabel klasy RG6, zasięg można znacznie zwiększyć.

W skład serii N kamer 8-megapikselowych wchodzi: kamera kompaktowa TWN-83IR o stałym obiektywie 3,6 mm, kamera kopułkowa TVN-81IR o stałym obiektywie 3,6 mm, kamera kopułkowa TVN-81MR wyposażona w obiektyw moto-zoom z autofokusem 3,3...12 mm.

Wyłącznym przedstawicielem firmy MAZi Security Systems GmbH jest GDE Polska.

HIKVISION www.hikvision.com/pl

Bezdotykowy terminal Hikvision DS-K5604A-3XF/V

Rozszerzeniem możliwości kamer termowizyjnych Hikvision są autonomiczne terminale pomiarowe Hikvision MinMoe, łączące funkcje kompaktowego monitora LCD, kamery termowizyjnej i kontrolera dostępu do pomieszczeń.

W zależności od modelu mogą mieć budowę kompaktową do montażu na ścianie, bądź jako lekki przenośny stojak ustawiany np. przy wejściu lub w ciągach komunikacyjnych. Wymagają jedynie podłączenia zasilania i opcjonalnie sieci komputerowej. Każda osoba podchodząca do terminala widzi swoją twarz na ekranie, w tym czasie wykonywany jest pomiar temperatury. Komunikat głosowy i wizualny potwierdza możliwość wejścia.

Terminal potrafi też wykryć, czy osoba nosi maseczkę. Jeśli zostanie zainstalowany przy drzwiach wejściowych, automatycznie może je zablokować, gdy badana osoba ma podwyższoną temperaturę lub nie nosi maseczki. Dostępna jest też funkcja szybkiego (poniżej 0,2 s) rozpoznawania twarzy (możliwość porównania obrazu z kamery z bazą danych obejmującą do 50 tys. osób). Dzięki zastosowaniu algorytmów AI bezbłędnie rozpoznaje osoby z bazy mimo założonych maseczek. System także automatycznie kontroluje wej-



ścia do budynku, sprawdzając, czy osoba jest na liście uprawnionych. Ekran dotykowy LCD 10"; rozdzielczość wyświetlacza 1024 x 600; odległość odczytu 0,3 do 2 m; szybki tryb pomiaru temperatury – wykrywanie twarzy i pomiar bez zapisu cech identyfikacyjnych; zakres pomiaru 30 do 45°C; dokładność +/- 0,5°C (bez ciała czarnego); pojemność 100 tys. zdarzeń.

POLON-ALFA



PROJEKTUJEMY *zgodnie ze sztuką*

SYSTEMY SYGNALIZACJI POŻAROWEJ

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

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A.

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



PRODUKT NUMERU

LINC POLSKA www.linc.pl

KENTIX SmartXcan – inteligentny pomiar temperatury i kontrola dostępu

Jednym z objawów choroby zakaźnej jest podwyższona temperatura ciała, dlatego poszukujemy rozwiązań, które ją wykrywają, a przy tym szybko i bezpiecznie identyfikują osoby chore.

Niemiecka firma KENTIX stworzyła SmartXcan do dokładnego, szybkiego i zgodnego z regulacjami RODO bezdotykowego pomiaru temperatury ludzkiego ciała. Czerwona dioda na interfejsie automatycznie informuje o podwyższonej temperaturze, zielona oznacza, że jest ona w normie. Urządzenie może działać niezależnie, można je też zainstalować przy wejściach do obiektu i zintegrować

np. z automatycznymi drzwiami, bramkami, by blokować wstęp osobom z gorączką. Ponad 1000 punktów pomiarowych oraz algorytmy sztucznej inteligencji gwarantują uzyskiwanie dokładnych, odpornych na manipulację wyników. Urządzenie można też wyposażać w czytnik RFID, który pozwoli na identyfikację osoby mającej prawo dostępu oraz ewidencję czasu wejść i wyjść z obiektu.

KENTIX SmartXcan szybko identyfikuje osoby chore, dzięki czemu można ograniczyć rozprzestrzenianie się wielu chorób zakaźnych. Sprawdzi się w szpitalach, instytucjach publicznych, fabrykach, klubach sportowych, biurach i obiektach rekreacyjnych, a to tylko przykładowe obszary jego zastosowań. Jest prosty w instalacji i użytkowaniu, a kolejnym jego atutem jest bardzo atrakcyjna cena. Zachęcamy do wzięcia udziału w bezpłatnych seminariach online, więcej na www.linc.pl/szkolenia.



SCHRACK SECONET POLSKA www.schrack-seconet.pl

Integral Remote – narzędzia zdalnego dostępu

Integral Remote to pakiet aplikacji IP pozwalających na zdalne nadzorowanie, zarządzanie oraz obsługę systemów sygnalizacji i pożarowej firmy Schrack Seconet. Jego zalety dostrzegają zarówno inwestorzy, zarządcy, integratorzy, jak i osoby obsługujące i serwisujące instalacje sygnalizacji pożarowej.



Wszystkie dane oraz dostęp do aplikacji są chronione wielopoziomowo, a dodatkowe bezpieczeństwo zapewnia realizowanie wszystkich połączeń w ramach pakietu poprzez połączenia szyfrowane oraz certyfikowane tunele VPN.

W SKŁAD PAKIETU WCHODZĄ:

1. Integral Application Center – pakiet przeznaczony dla programistów i instalatorów systemu Integral IP.
2. Integral Desktop – przeznaczony do obsługi oraz nadzorowania instalacji na komputerach stacjonarnych. Program wyświetla odwzorowany 1:1 panel obsługi centrali sygnalizacji pożarowej Integral IP.
3. Integral Mobile/Integral Browser – aplikacja odwzorowuje panel centrali Integral IP na urządzeniach mobilnych oraz wspiera technologię aktywnych powiadomień (*push notification*).
4. Integral Message – przeznaczony do zdalnego nadzorowania wielu niezależnych instalacji sygnalizacji pożarowej Integral IP podłączonych do serwera systemu, który wraz ze stanowiskami operatorskimi stanowi centrum nadzoru.
5. Integral Mail – umożliwia wysyłanie e-maili bezpośrednio z centrali SSP, która łącząc się z dedykowanym serwerem pocztowym, wysyła informacje o najważniejszych zdarzeniach w systemie Integral IP.

TP-LINK www.tp-link.com.pl

TP-Link CPE710 – kierunkowa antena do transmisji na długie dystanse w paśmie 5 GHz

TP-Link wprowadza do oferty nowe urządzenie służące do połączeń Wi-Fi punkt-punkt lub punkt-wielopunkt na duże odległości. CPE710 pracuje w standardzie 802.11ac (Wi-Fi 5) i zapewnia prędkość transmisji bezprzewodowej do 867 Mb/s w paśmie 5 GHz.

Model CPE710 wyposażony w moduł radiowy w paśmie 5 GHz i antenę o wysokim zysku (aż 23 dBi) oferuje stabilną transmisję danych na duże odległości. Zaletą jest opcja regulacji mocy sygnału zależnie od rodzaju połączeń (*point-to-point* lub *point-to-multipoint*).

Oprócz funkcji punktu dostępowego CPE710 może też pracować w trybie klient/router AP

(klient WISP), router AP oraz klient AP. By zapobiec kolizjom pomiędzy punktami CPE, urządzenie korzysta z technologii TP-Link MAXtream TDMA. Technologia 2x2 MIMO zwiększa wydajność sieci bezprzewodowej.



Instalacja urządzenia jest prosta (dołączony zestaw montażowy, elementy zatrzaskowe). Solidna konstrukcja gwarantuje stabilność anteny nawet przy dużym wietrze. Obsługa pasywnego PoE daje swobodę wyboru lokalizacji (dołączony pasywny adapter PoE).

Obudowa urządzenia (IP65) chroni przed deszczem i śniegiem, gwarantuje odporność na niskie i skrajnie wysokie temperatury (-40...70°C). Administratorzy sieci docenią bezpłatne oprogramowanie do zarządzania z jednego komputera urządzeniami CPE710 w sieci. System Pharos Control umożliwia personalizację ustawień i oferuje m.in. wykrywanie urządzeń, monitorowanie stanu, aktualizację oprogramowania, konserwację sieci.

KENTIX
Innovative Security

Linc
Polska Sp. z o.o.

NOWE PODEJŚCIE DO POMIARU TEMPERATURY



Identyfikacja
osób zakażonych



Pomiar
temperatury



Jedna prosta metoda,
wiele zastosowań



RODO

Zgodność
z RODO



KENTIX
SmartXcan

- ✓ BEZPIECZNIE
- ✓ INTUICYJNIE
- ✓ SZYBKO

NOWOŚĆ

www.linc.pl/kentix-smartxcan



BEZPIECZEŃSTWO BIZNESU

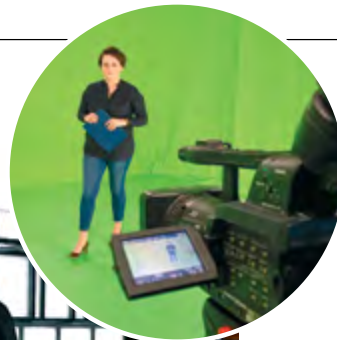


JAKIE BRANŻE SĄ OKRADANE?

“Bezpieczny Biznes” to nowy i jedyny w polskiej telewizji program dotyczący tej tematyki. Magazyn jest emitowany w telewizji BIZNES24 oraz online. To autorska produkcja redakcji “a&s Polska”.

BEZPIECZNY BIZNES

premiera naszego programu
w BIZNES24



- Premiera w BIZNES24 w każdy piątek o 10:30
- Premiera online w każdy poniedziałek o 10:30 (na portalu aspolska.pl oraz naszym kanale na YouTube)

W pierwszym odcinku o bezpieczeństwie w handlu rozmawiamy z ekspertem ds. bezpieczeństwa Mirosławem Lukowskim, o business resilience opowiada Grzegorz Ćwiek z Instytutu Bezpieczeństwa RESCON, a na temat problemu wewnętrznego złodzieja w firmie mówi Jacek Grzechowiak z Securitas Polska. Program prowadzi Jolanta Kucharska z a&s Polska. □



BEZPIECZEŃSTWO HANDLU?



KTO MUSI BYĆ GOTOWY NA KRYZYS?

BIZNES24



BEZPIECZNY
BIZNES

PREMIERA W TV BIZNES24
w każdy piątek o 10:30

PREMIERA ONLINE
w każdy poniedziałek o 10:30
na portalu aspolska.pl
oraz na kanale a&s Polska
na YouTube





Plany awaryjne na wypadek wystąpienia koronawirusa w CMA

Jakie działania należy podjąć, aby ograniczyć ryzyko przerwania ciągłości pracy centrum monitorowania alarmów związane ze skutkami zarażenia operatorów koronawirusem SARS-CoV-2, który wywołuje chorobę COVID-19?



T E K S T

Daniel Kamiński

Centrum Monitorowania Alarmów powinno z założenia działać w sposób ciągły. W obecnej sytuacji ryzyko zakażenia operatorów koronawirusem SARS-CoV-2 powoduje, że ciągłość działania CMA jest zagrożona. Skala pandemii sprawia, że jest to jedno z największych zagrożeń dla firm świadczących usługi monitorowania alarmów. Wystarczy, że któryś z pracowników okaże się chory i... jest problem. Obsługa centrum zostanie poddana kwarantannie, a pomieszczenia będą wymagały dezynfekcji.

Analiza zagrożeń CMA

Rolą Centrum Monitorowania Alarmów jest zbieranie informacji z chronionych obiektów i podejmowanie działań w przypadku wystąpienia alarmu. Unieruchomienie CMA spowodowałoby brak reakcji służb ochrony na zdarzenia alarmowe. Mówiąc wprost, w przypadku alarmu nikt nie wyśle załogi interwencyjnej, serwisu czy też nie wezwie policji. Z tego powodu każde centrum monitorowania powinno przeprowadzić analizę zagrożeń. Jej posiadanie jest również jednym z wymagań opisanych w normie PN-EN 50518 dedykowanej dla CMA. W ramach analizy zagrożeń dokonuje się przeglądu procesów krytycznych występujących w CMA i analizuje, jak mogą na nie wpłynąć zidentyfikowane zagrożenia. Najczęściej uwagę skupia się na zagrożeniach kryminalnych, terrorystycznych i technicznych, w mniejszym stopniu szacuje się ryzyko zagrożeń zdrowotnych, m.in. epidemii czy pandemii.

Epidemia COVID-19 wiele zmieniła w zakresie analizy zagrożeń. Sposób przenoszenia się wirusa, szybko rosnąca liczba chorych oraz uciążliwość objawów wywołały wiele ograniczeń w świadczeniu usług. Obecne obostrzenia urzędowe dotyczące organizacji pracy zmuszają do przebudowy stanowisk operatorskich lub pracy zdalnej operatorów. Największym ryzykiem jest jednak możliwość wprowadzenia kwarantanny dla personelu. Jak dużo firm świadczących usługi ochrony jest przygotowanych na zamknięcie centrum monitoringu z tego powodu? Odpowiedź jest zadowalająca, w mojej ocenie większość firm posiadających CMA wprowadziła działania awaryjne na taką okoliczność. Poniżej przedstawiono najczęściej stosowane działania zapobiegawcze i awaryjne.

Plany awaryjne

Plany awaryjne wykonuje się w celu przygotowania centrum monitoringu do sytuacji kryzysowych. Zakres działań zależy od prawdopodobieństwa wystąpienia zdarzenia kryzysowego oraz stopnia niedostępności zasobów. Inne działania zostaną podjęte w trakcie pożaru budynku, w którym znajduje się centrum monitoringu, a inne w przypadku awarii programu obsługi alarmów. Plany awaryjne na wypadek zagrożenia koronawirusem w tym artykule zostaną ograniczone do obsady centrum monitoringu.

Działania zapobiegawcze

W celu uniknięcia kryzysu można podjąć kilka działań zapobiegawczych. Z pomocą przychodzi zasada ograniczonego dostępu do centrum monitoringu. Do CMA nie powinny mieć dostępu osoby postronne, więc ryzyko zarażenia się wirusem jest mniejsze niż np. w biurze. Wprowadzenie środków dezynfekcyjnych, wdrożenie procedury odkażania stanowisk w trakcie przejmowania dyżuru obniża ryzyko zachorowania. Zastosowanie się do zaleceń oddalenia od siebie stanowisk roboczych jest kolejnym działaniem prewencyjnym planów awaryjnych.

Plany awaryjne na wypadek kwarantanny

Operatorzy CMA mogą się zarazić wirusem w domu lub w drodze do pracy. Na szczęście na taką sytuację również można się przygotować. Jednym z rozwiązań jest skorzystanie z zapasowego centrum monitoringu. Jeśli go nie ma, można takie centrum uruchomić w biurze, gdyż większość pomieszczeń jest obecnie pusta. Korzystając z dwóch centrów monitoringu, należy pilnować, żeby obsada była przypisana tylko do jednej lokalizacji. Mieszanie się operatorów między lokalizacjami podnosi ryzyko zarażenia się. Można też uruchomić pracę zdalną operatorów, co znacząco ogranicza prawdopodobieństwo, że kwarantanna pracowników centrum uniemożliwi świadczenie usług monitorowania alarmów. Wymaga jednak zainwestowania w laptopy i przenośne systemy komunikacji. Dla firm korzystających z narzędzi pracujących w chmurze sposób ten jest prostszy do realizacji. Inną metodą przygotowania się na wypadek kwarantanny pracowników jest podpisanie umowy z zewnętrznym centrum monitoringu. Wtedy w sytuacji kryzysowej sygnały alarmowe i telefony są przekierowywane właśnie do niego.

Rola technologii w planach awaryjnych

Każdy z omówionych planów awaryjnych wymaga inwestycji w infrastrukturę techniczną. Z doświadczenia mogę powiedzieć, że najpopularniejsze programy obsługi alarmów pozwalają na wszystkie trzy wymienione plany awaryjne, czyli równoległą pracę w dwóch (lub więcej) centrach monitoringu, zdalną pracę operatorów oraz przekierowanie obsługi zdarzeń do zewnętrznego centrum.

Od poziomu wyszkolenia obsady technicznej oraz dostępnych narzędzi zależy, jak dużą przerwę w świadczeniu usług monitorowania alarmów spowoduje uruchomienie konkretnego planu awaryjnego. Krótka przerwa może być niezauważalna dla klientów, ale przerwa kilkugodzinna czy kilkudniowa może spowodować zerwanie umów.

Plany ciągłości działania CMA

Planując awaryjną pracę centrum monitorowania, należy założyć czasowe ograniczenie zakresu świadczonych usług. Przy pracy zdalnej lub przekierowaniu obsługi do zewnętrznego centrum monitoringu może się okazać, że np. nie ma wszystkich informacji niezbędnych do świadczenia usług dodanych. Wtedy należy skoncentrować się na usługach podstawowych do momentu utworzenia zasobów.

Choroba operatorów może doprowadzić do czasowego ograniczenia obsady, co warto przewidzieć w planie ciągłości działania. W takiej sytuacji można wprowadzić nadgodziny, zmienić tryb pracy, wzmocnić obsadę w godzinach największego ruchu lub skorzystać z wynajmu pracowników.

Sytuacja kryzysowa w CMA

W przypadku sytuacji awaryjnej powinno się powołać sztab kryzysowy. Jego rolą będzie uzgodnienie zasady współpracy kryzysowej z patrolami interwencyjnymi i działem serwisu. Sztab kryzysowy może wprowadzać w życie plany awaryjne w zależności od sytuacji. Istotnym elementem będzie powiadomienie klientów o zaistniałej sytuacji kryzysowej i podjętych środkach zaradczych. Warto utrzymywać kontakt z klientami, gdyż to oni mogą pomóc przejść przez kryzys lub go spotęgować.

Szkolenie organizowane przez PISA

Omówione zagrożenia i dostosowane do nich plany awaryjne stanowią mały fragment rozważań na temat możliwych zagrożeń występujących w centrum monitoringu. Mogą być one ograniczane dzięki czynnościom podejmowanym w ramach planów ciągłości działania. Więcej informacji na ten temat można uzyskać podczas szkolenia *Monitoring alarmów i zdalny dozór wizyjny* organizowanego przez Polską Izbę Systemów Alarmowych (PISA), którego jestem pomysłodawcą. ▣

B I O

Daniel Kamiński

Absolwent kierunku Telekomunikacji WAT oraz Kierowania Systemami Teleinformatycznymi AON. Od 1995 r. w branży zabezpieczeń technicznych związany z monitoringiem alarmów. Pierwsze 10 lat w grupie AAT/CMA odpowiadał za utrzymanie ciągłości działania centrum monitorowania oraz wsparcie sprzedażowe, następnie w międzynarodowych firmach G4S i ADT. W ostatnich latach jako doradca wykorzystywał swoje doświadczenie wdrażania nowych produktów i usług w firmach Juventus oraz EBS. Od ponad 20 lat dzieli się swoją wiedzą na łamach czasopism branżowych.



Ultraszybka infostrada szerokopasmowa

DZISIAJ TRUDNO SOBIE WYOBRAZIĆ MIASTA, KTÓRE MOGĄ SIĘ ROZWIJAĆ BEZ ODPOWIEDNIEJ INFRASTRUKTURY, W TYM RÓWNIEŻ TELEKOMUNIKACYJNEJ, ZAPEWNIAJĄCEJ PEWNĄ I SZYBKĄ WYMIANĘ INFORMACJI. USŁUGI SMART CITIES BAZUJĄ PRZEWAŻNIE NA INFORMACJACH PRZESTRZENNYCH PRZETWARZANYCH W CZASIE RZECZYWISTYM I DOTYCZĄ WIELU SFER ŻYCIA MIESZKAŃCÓW MIASTA.

Znaczna część usług opartych na wymianie danych mieści się w takich obszarach, jak inteligentne zarządzanie ruchem (komunikacja miejska i ruch drogowy, reagowanie w czasie rzeczywistym na codzienne wydarzenia, np. zatory komunikacyjne), optymalizacja oraz śledzenie zużycia i przesyłania energii, monitoring zanieczyszczenia powietrza i jakości wody, gospodarka odpadami, zarządzanie infrastrukturą w miastach, telemedycyna, bezpieczeństwo.

Choć miasto kojarzy nam się z infrastrukturą kablem zapewniającą dostęp do Internetu, to jednak ponad 90% z nas korzysta również z Internetu mobilnego dostępnego w telefonie. Także miliony urządzeń równolegle korzystają z bezprzewodowego dostępu do sieci. Aż trudno w to uwierzyć, ale w 2018 r. operatorzy w Polsce zarządzali ponad 51 milionami aktywnych kart SIM¹. Już wtedy wieszczono, że dalszy wzrost aktywnych urządzeń wykorzystujących mobilny dostęp do Internetu spowoduje, że sieć LTE (4G) się zatka². Transmisja danych w sieciach mobilnych jest od kilku lat najbardziej dynamicznie rozwijającą się usługą. Poprzez urządzenia mobilne dwa lata temu przesłano łącznie 3098 PB (3 098 106 GB) danych. W ujęciu statystycznym na jednego Polaka w 2018 r. przypadło średnio 84,6 GB³. Instytut Łączności – Państwowy Instytut Badawczy prognozuje, że średni miesięczny popyt na dane (wysyłanie i odbiór danych) w urządzeniach mobil-

nych w Polsce wzrośnie do 2025 r. prawie 25-krotnie⁴. To wyzwanie dla sieci bezprzewodowych, które pomimo istniejącej infrastruktury kablowej są najchętniej wybierane przez użytkowników Internetu.

Te wyniki stają się jeszcze ciekawsze, gdy zestawimy je z prędkością transferów sieci LTE, a te sytuują Polskę na końcu krajów europejskich⁵. Powodem tego stanu rzeczy były przyjęte bardzo niskie limity poziomów pól elektromagnetycznych (100 razy mniejsze natężenie pola elektrycznego niż w innych krajach) jeszcze z czasów istnienia Związku Radzieckiego, oparte na założeniach sprzed okresu dostępności telefonu komórkowego, kiedy dysponowano znacznie mniejszą niż obecnie wiedzą nt. pól elektromagnetycznych⁶. Ograniczenia gęstości mocy na poziomie 0,1 W/m² (7 V/m) negatywnie wpłynęły na efektywność i elastyczność budowy Stacji Bazowych Telefonii Komórkowej (SBTK), współdzielenie lokalizacji dedykowanych dla instalacji antenowych oraz na gospodarowanie (na podstawie pozwoleń) zasobami częstotliwości wykorzystywanych w sieciach komórkowych 4G. Przełożyło się to na szybkość Internetu 4G, która w Polsce nadal jest najmniejsza w całej Europie (ok. 30 Mb/s – pobieranie, 8 Mb/s – wysyłanie, w porównaniu np. z 42/15 Mb/s w Czechach, nie wspominając o wynikach w Holandii 76/16⁶), pomimo że nakłady inwestycyjne polskich operatorów na rozwój infrastruktury kształtowały się na poziomie średniej europejskiej⁷.

Dlatego też w grudniu ub.r. ministrowie zdrowia i cyfryzacji podpisali rozporządzenie wprowadzające wyższe limity poziomów pól elektromagnetycznych w Polsce⁸, harmonizujące wymagania środowiskowe w Polsce (tzw. normy PEM) z obowiązującymi limitami w UE zgodnie z zaleceniem 1999/519/WE. W praktyce oznacza to, że wcześniejszy limit gęstości mocy 0,1 W/m² został zwiększony do 10 W/m² (61 V/m w zakresie częstotliwości od 2 do 300 GHz). Ten zabieg pozwoli operatorom uruchomić zarówno sieć 5G, jak i nowe pasma LTE bez zmniejszania mocy obecnych nadajników 4G. I dzięki temu Internet mobilny w Polsce będzie szybszy.

- 1) <https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/uke-internet-stacjonarny-cena-telewizja-telefon-raport>
- 2) „Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r.” UKE, czerwiec 2019, Warszawa
- 3) „Czy Polska grozi blackout mobilnego internetu?” Polska Izba Informatyki i Telekomunikacji, Warszawa 8.03.2019
- 4) „Raport o stanie rynku telekomunikacyjnego w Polsce w 2018 r.” UKE, czerwiec 2019, Warszawa
- 5) „Czy Polska grozi blackout mobilnego internetu?” Polska Izba Informatyki i Telekomunikacji, Warszawa 8.03.2019
- 6) Speedtest Global Index, kwiecień 2020
- 7) „Oddziaływanie elektromagnetycznych fal milimetrowych na zdrowie pracowników projektowanych sieci 5G i populacji generalnej” Narodowy Program Zdrowia, pod redakcją prof. dr. hab. med. Konrada Rydzynskiego, Łódź 2019



T E K S T

Jan T. Grusznicki

Czym jest 5G?

5G to skrót od „Piąta Generacja” bezprzewodowej technologii i jest kolejną, po 4G (LTE), ewolucją technologii komórkowej ustandaryzowaną przez 3rd Generation Partnership Project (3GPP) – międzynarodową organizację normalizacyjną mającą na celu rozwój systemów telefonii komórkowej. 5G zapewnia skokowo większą szybkość, poprawia wydajność i przepustowość sieci, a operatorom umożliwia rozwiązanie problemu gwałtownego wzrostu liczby połączeń z urządzeń mobilnych i IoT.

Mniej więcej co dziesięć lat technologia mobilna nowej generacji przynosi przełomową poprawę wydajności oraz wprowadza nowe aplikacje i możliwości zastosowań. W latach 80. XX wieku analogowa telefonia komórkowa umożliwiała rozmowy telefoniczne. W latach 90. sieć 2G (GSM) wprowadziła digitalizację połączeń i wysyłanie wiadomości tekstowych SMS. Na przełomie XX i XXI wieku technologia 3G (UMTS) wprowadziła mobilny Internet, strumieniowe przesyłanie muzyki i wiadomości obrazkowych. A w 2010 r. 4G LTE zapewniło wystarczającą pojemność, aby umożliwić prawdziwie multimedialne wrażenia, w tym strumieniowe przesyłanie wideo HD.

Sieć 5G jest czasami określana jako 5G NR, co oznacza Nowe Radio (ze względu na użytą technologię dostępu radiowego), które będzie wykorzystywać dwa zakresy częstotliwości: zakres częstotliwości 1 (FR1), w tym zakresy poniżej 6 GHz, oraz zakres częstotliwości 2 (FR2), w tym zakresy częstotliwości w zakresie fal milimetrowych (24...100 GHz)⁹. Więcej częstotliwości oznacza większą pojemność, większą liczbę obsługiwanych użytkowników oraz większe prędkości transferu danych.

W Polsce sieć 5G ma korzystać z pasma 700 MHz, obecnie wykorzystywanego przez cyfrową telewizję naziemną¹⁰, w zakresie częstotliwości 3,4...3,8 GHz, który zapewni większy zasięg niż obecnie ma sieć 4G LTE (od dekady jest używany powszechnie w urządzeniach szerokopasmowego radiowego przesyłu danych typu

- 8) Speedtest Global Index, kwiecień 2020
- 9) „Wpływ limitów gęstości mocy (PDL – Power Density Limits) na łączność bezprzewodową: czy Polska grozi opóźnieniami w rozwoju 5G?” M. Godlewski, M. Steiger, R. Schicht, H. T. Bernold, BCG, lipiec 2018
- 10) Rozporządzenie Ministra Zdrowia z 17 grudnia 2019 r. w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku, Dz.U. 2019 poz. 2448
- 11) http://www.sharetechnote.com/html/5G_FR_Bandwidth.html (2020-06-02)
- 12) Zapewnia dobrą wydajność sieci wewnątrz budynków i dobry zasięg. Ponieważ fale na tych częstotliwościach rozchodzą się równomiernie i z powodzeniem pokonują przeszkody architektoniczne, są w stanie pokryć terytorium całego kraju.

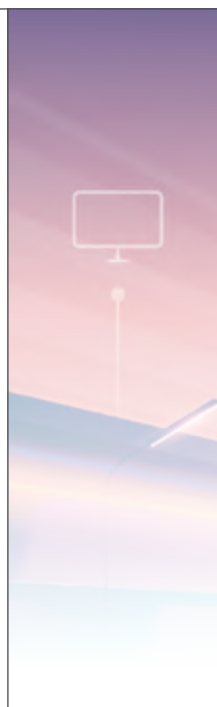


Wimax¹³⁾, a nawet 26 GHz – najwyższą częstotliwość, jaką do tej pory zastosowano w sieciach komórkowych, zapewniającą prędkości osiągane przez światłowód¹⁴⁾.

Docelowo wiele stacji bazowych, stanowiących element architektury 5G, będzie miało mniejszą moc niż stacje stosowane dzisiaj, a sieć, aby sprawnie działać, będzie potrzebowała ich o wiele więcej. Szacuje się, że docelowe pełne wdrożenie sieci 5G pracującej na falach o częstotliwości 26 GHz będzie potrzebować nawet do 100 razy więcej nadajników¹⁵⁾. Jednak w pierwszej fazie budowy sieci 5G zostaną wykorzystane obecne częstotliwości 3400...3800 MHz oraz tzw. pasmo 700 MHz (nastąpi migracja z 3G, 4G LTE do 5G), co jeszcze nie przełoży się na znacząco większą liczbę nadajników.

Spełnienie wysokich wymagań stawianych przed 5G, w szczególności w zakresie przepływności transmisji danych (*down-link* 20 Gb/s, *up-link* 10 Gb/s)¹⁶⁾, czy małych opóźnień (ok. 4 ms¹⁷⁾), wymusza połączenie SBTK nowej generacji za pomocą światłowodów. To diametralna różnica wobec sieci 2G – 4G, gdyż w ich topologii dominowały miedziane łącza o przepływności E1, a następnie radiolinie tzw. gęstych sieci rozumianych jako zastosowanie wielu stacji bazowych o krótkich zasięgach znacznie zwiększy efektywność widmową, a zatem przepływność oferowaną klientowi. W sieci 5G odchodzi się od sieci stacji bazowych dużych rozmiarów na rzecz sieci składających się z dużej liczby małych nadajników¹⁸⁾.

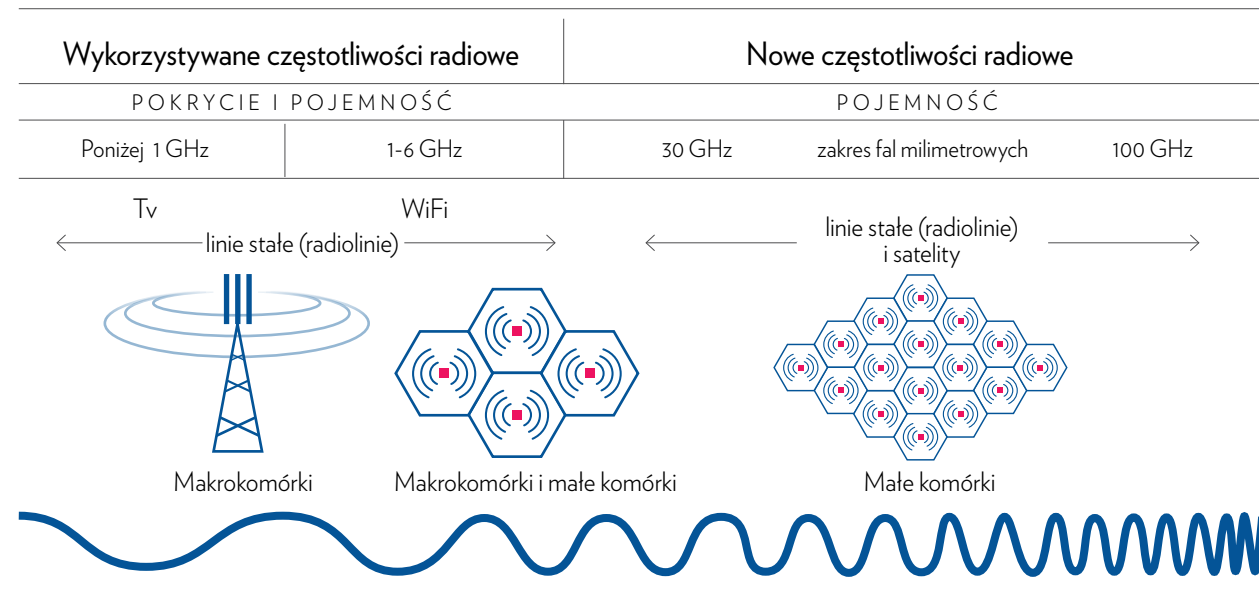
Zmieni się również system antenowy. W tradycyjnym moc jest promieniowywana w szerokim zakresie wg ustalonej charakterystyki przestrzennej. Obszar, w którym mogą znajdować się użytkownicy, jest z góry zdefiniowany. W antenie aktywnej sieci 5G z Massive MIMO moc jest promieniowana w określonych kierunkach, skupionych na indywidualnych użytkownikach lub ich grupach, rzadko zlokalizowanych w obszarze usług. Kierunki promieniowania mocy mogą zmieniać się niemal automatycznie, by skupić się na ruchomych użytkownikach lub obiektach i ograniczyć zakłócenia dla innych¹⁹⁾. Anteny Massive MIMO stanowią kluczowy element architektury sieci piątej generacji. Ich działanie można sprowadzić do zasa-



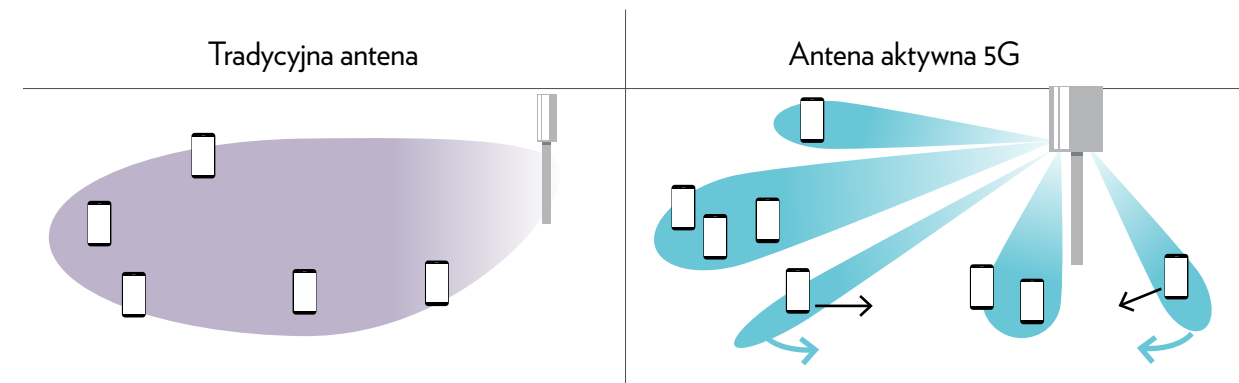
dy, zgodnie z którą sieć umożliwia transmisję i odbiór więcej niż jednego sygnału jednocześnie. Standardowe anteny MIMO zakładają użycie dwóch lub czterech anten, Massive MIMO natomiast przewiduje istnienie kilkudziesięciu (niektóre firmy zaprezentowały systemy Massive MIMO z ponad 100 antenami), które są jednak o wiele mniejsze od standardowych. W im więcej anten wyposażono nadajnik i odbiornik, tym oferują one więcej możliwych ścieżek sygnału i lepszą wydajność pod względem zarówno szybkości transmisji, jak i niezawodności łącza. Co więcej, zastosowanie większej liczby anten spowoduje również większą odporność na celowe zakłócenia w sieci. Anteny Massive MIMO będą wykorzystywały technologię inteligentnego kształtowania wiązki radiowej, która umożliwi ukierunkowanie widma (tzw. *beamforming*) w stronę określonego odbiornika. Sygnał będzie przetwarzany w taki sposób, aby tra-

- 13) Wydajność wewnątrz budynków może być nieco niższa niż w przypadku poprzedniej generacji technologii.
14) Problemem jest jednak ograniczenie zasięgu przez tłumienie powodowane choćby liśćmi drzew i krzewów, nie wspominając o takich przeszkodach, jak ściany budynków czy ukształtowanie terenu. Szacowane zasięgi w ramach tego pasma wynoszą od 50 do 500 m w przestrzeniach otwartych, natomiast w obszarach zabudowanych nie przekraczają 200 m.
15) „Stacje Bazowe”, Ministerstwo Cyfryzacji, <https://www.gov.pl/web/5g/stacje-bazowe> (2020-06-03)
16) Minimum requirements related to technical performance for IMT-2020 radio interface(s)”, ITU-R M.2410-0, listopad 2017
17) Tamże
18) „Krótka opowieść o społeczeństwie 5.0. Czyli jak żyć i funkcjonować w dobie gospodarki 4.0 i sieci 5G. Załącznik 2, Uwarunkowania techniczne rozwoju sieci 5G”. Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, Fundacja Digital Poland
19) Tamże

Częstotliwości dla 5G



RYS. 1. Częstotliwości dla 5G, inne usługi bezprzewodowe (TV, Wi-Fi, łącza stałe i satelitarne) pokazano dla porównania. Źródło: EMF Explained Series, 5G and EMF Explained, marzec 2018



RYS. 2. Stacje bazowe – Sektorowa stacja bazowa 4G – stacja bazowa 5G z Massive MIMO. Źródło: „Krótka opowieść o społeczeństwie 5.0. Czyli jak żyć i funkcjonować w dobie gospodarki 4.0 i sieci 5G. Załącznik 2, Uwarunkowania techniczne rozwoju sieci 5G” Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji, Fundacja Digital Poland

fić do użytkownika w formie ukierunkowanego sygnału. Do każdego użytkownika lub grupy użytkowników znajdujących się na danym azymucie będzie docierała osobna, dedykowana dla niego wiązka sygnału, co zapewni wysoką stabilność połączenia²⁰⁾. Sieć radiową 5G cechują bardzo niskie opóźnienia, ale mimo to całkowite opóźnienia w komunikacji, z wykorzystaniem tradycyjnych serwerów, nadal mogą być nieakceptowalne w takich aplikacjach, jak pojazdy autonomiczne. Wynika to z faktu, że przetwarzanie informacji najczęściej odbywa się daleko od użytkownika, w dedykowanych serwerowniach.

By sieć 5G mogła obsłużyć takie przypadki, przetwarzanie danych musi być zlokalizowane jak najbliżej miejsca ich zbierania, co zminimalizuje opóźnienia związane z transmisją danych przez sieć. Właśnie w tym celu została opracowana przez ETSI (Europejski Instytut Norm Telekomunikacyjnych) koncepcja *Multi-Access Edge Computing*, zwana poprzednio *Mobile Edge Computing* (MEC). MEC to koncepcja architektury sieci 5G, która umożliwia przetwarzanie w chmurze na obszarach sieci radiowej. Podstawową ideą stojącą za MEC jest skrócenie odległości komunikacji –

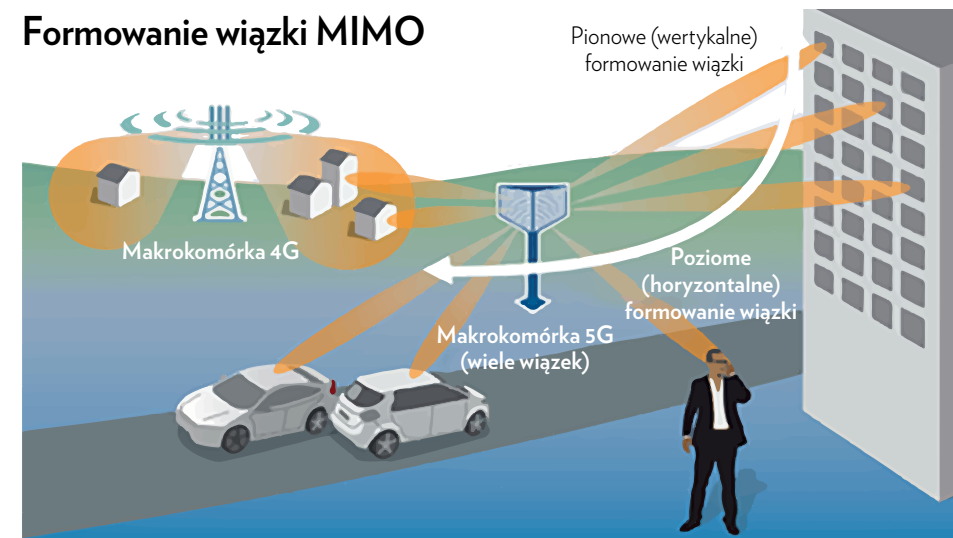
uruchamianie aplikacji i wykonywanie związanych z nimi obliczeń bliżej użytkownika sieci komórkowej. MEC zmniejsza też obciążenie sieci szkieletowej i dzięki temu aplikacje osiągają lepsze wyniki. Technologia MEC ma być wdrażana w SBTK lub innych węzłach brzegowych, umożliwiając elastyczne i szybkie stosowanie nowych aplikacji i usług dla użytkowników. MEC, w porównaniu z chmurą obliczeniową, charakteryzuje bliskość i lokalność obliczeń, niższe opóźnienia oraz znajomość kontekstu sieciowego i lokalizacji²¹⁾.

Jakie zastosowania ma 5G?

Potencjalne zastosowania sieci 5G wynikają przede wszystkim z możliwości obsługi bardzo dużej liczby urządzeń o niskim poborze mocy oraz wprowadzenia tzw. ultraniezawodnej transmisji o małych opóźnieniach. Te dwie cechy 5G otwierają drzwi do nowych zastosowań sieci komórkowej oraz znaczącego rozwoju zastosowań istniejących. Sieć 5G ma zapewnić kolejny krok w całkowitej transformacji przemysłu, technologia 5G zrewolucjonizuje obszar ochrony zdrowia i usług medycznych, zwłaszcza telemedycyny. Potencjalne możliwości jej wpływu na ochronę środowiska w znacznej mierze wynikają bezpośrednio z rozwoju usług IoT i *smart cities*, bazujących na wszelkiego rodzaju bezprzewodowych sensorach.

W najszerszym ujęciu sieć 5G może mieć korzystny wpływ na czystszy, bardziej ekologiczny i przyjazny środowisku przyszłość, zwiększając wydajność wielu procesów. Przykładami konkretnych zastosowań, które będą rozwijane wraz

Formowanie wiązki MIMO



RYS. 3. Formowanie wiązki MIMO Źródło: EMF Explained Series, 5G and EMF Explained, marzec 2018

20) 5G: Sieci Telekomunikacyjne Nowej Generacji, Ministerstwo Cyfryzacji [online:] <https://www.gov.pl/web/5g/inteligentne-nadajniki> (2020-05-28)

21) „5G. Szanse, zagrożenia, wyzwania” F. Felici, A.G. Rodriguez, P. Mieczkowski, K. Mikulski, T. Piekarz, B. Sztokfisz, redakcja R. Siudak, Instytut Kościuszki, Kraków 2020

Porównanie 5G z 4G²²

5G

4G

PRĘDKOŚĆ SZCZYTOWA

10

GIGABITÓW / S

1,45

GIGABITÓW / S

W porównaniu z obecną czwartą generacją, 5G może osiągnąć ponad 6-krotnie większą przepustowość. Większe prędkości otwierają drzwi przed nowymi możliwościami sieci komórkowych. Aplikacje wymagające do pracy dużej ilości danych w urządzeniach końcowych, np. pobieranie wielogigabajtowych plików i strumieniowe przesyłanie wideo 4K/8K, mogą stać się rzeczywistością.

OPÓŹNIENIE

<10

MILISEKUND

40-50

MILISEKUND

Mrugnij oczami. Tak szybko dane mogą być przesyłane z Twojego przyszłego urządzenia z dostępem do sieci 5G, przez sieć do głównego serwera i z powrotem do urządzenia. To niezwykle małe opóźnienie – 4 do 5 razy szybciej niż w 4G – umożliwi korzystanie z aplikacji działających w czasie rzeczywistym, np. pojazdy autonomiczne, zaawansowana robotyka i rozszerzona rzeczywistość.

ŁĄCZNOŚĆ

1 milion

OBSŁUGIWANYCH URZĄDZEŃ / KM²

10K - 100K

OBSŁUGIWANYCH URZĄDZEŃ / KM²

5G może obsługiwać do 100 razy więcej urządzeń niż 4G – co prowadzi do tego, że świat będzie bardziej połączony niż kiedykolwiek. Zmiana ta ma kluczowe znaczenie, ponieważ już miliardy urządzeń IoT podłącza się do Internetu i obciąża istniejące sieci 4G. Pomyśl o 5G jako o rozwiązaniu, które stworzy w przyszłości miasta z inteligentnym transportem, efektywnymi sieciami energetycznymi i zdalnymi usługami bezpieczeństwa.

EFEKTYWNOŚĆ ENERGETYCZNA

90% mniej

ZUŻYTEJ ENERGII / 1 BIT

90% więcej

ZUŻYTEJ ENERGII / 1 BIT

Wstępne szacunki sugerują, że 5G może zużywać 90% mniej energii na bit niż 4G. Zużycie energii ma duży wpływ na żywotność baterii w urządzeniach przenośnych. Dla osób korzystających ze smartfonów, inteligentnych zegarków i tabletów jest to bolączką. Dzięki zastosowaniu szybkich sieci 5G o małym opóźnieniu więcej danych może być przetwarzanych w sieci, a nie w urządzeniu. Może to oznaczać mniejsze zużycie energii i dłuższą żywotność baterii.

WOLUMEN DANYCH MOBILNYCH

10

TERABAJTÓW / S / KM²

1/100

TERABAJTÓW / S / KM²

Wyobraź sobie obszary dużych skupisk ludzi, np. lotniska czy areny sportowe, na których tysiące urządzeń komunikuje się w tej samej sieci. Komunikacja raz po raz jest zrywana, a prędkość transferu danych drastycznie spada. Dzięki większym prędkościom i mniejszym opóźnieniom 5G może obsłużyć 1000 razy większą ilość danych mobilnych niż 4G.

z 5G i sprawniejszym działaniem czujników IoT, są np.: monitorowanie drgań i warunków materiałowych w budynkach, mostach czy zabytkach; monitorowanie natężenia hałasu w miastach oraz na ich obrzeżach w czasie rzeczywistym; monitorowanie lasów i terenów chronionych pod kątem pożarów; monitorowanie stanu powietrza, emitowanych zanieczyszczeń, stanu wód, poziomu opadów.

W obszarze bezpieczeństwa nowe rozwiązania obejmują zdalne systemy dozoru wizyjnego przesyłające strumienie wideo wysokiej rozdzielczości (8K i więcej) w czasie rzeczywistym. Monitoring wizyjny może objąć miejsca publiczne lub krytyczną infrastrukturę. Stanie się możliwe połączenie istniejących kamer np. z systemami rozpoznawania twarzy pozwalającymi na sprawną identyfikację osób zaginionych lub podejrzanych o popełnienie przestępstwa. Ten sam cel będzie miał system automatycznej detekcji zagrożeń, wykrywający podejrzane obiekty, anomalie lub zakłócenia w miejscach publicznych, a także zdarzenia atmosferyczne zagrażające obywatelom.

Czy 5G jest bezpieczne?

Pojawiło się wiele hipotez pseudonaukowych związanych z wprowadzanymi zmianami i sieciami 5G. Przykładem jest choćby podniesienie limitów natężenia pól elektromagnetycznych, co spowodowało naturalne obawy, czy taki zabieg jest bezpieczny dla zdrowia. Paradoksalnie zwiększenie limitu obniży ekspozycję ludzi na promieniowanie, gdyż to nasze telefony, a nie nadajniki są głównym źródłem promieniowania – im słabszy jest zasięg, tym wyższe promieniowanie emitowane przez telefon. Złagodzenie norm pozytywnie wpłynie na zasięg, ograniczając promieniowanie przez urządzenia mobilne²³.

Więcej na aspolska.pl

22) <https://datamakespossible.westerndigital.com/5g-vs-4g-side-by-side-comparison/>

23) „Pole elektromagnetyczne a człowiek. O fizyce, biologii, medycynie, normach i sieci 5G”, Ministerstwo Cyfryzacji, Instytut Łączności – Państwowy Instytut Badawczy, Warszawa 2019

B I O

Jan T. Grusznicki

Z-ca red. naczelnego „a&s Polska”. Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.



Sztuczna inteligencja w walce z pandemią



Kamera zmierzy temperaturę i prześle ostrzeżenie

Regularny pomiar temperatury jest jednym z najprostszych badań pozwalających wykryć gorączkę, która może świadczyć o infekcji wywołanej przez SARS-CoV-2. Tradycyjny termometr bezdotykowy nie sprawdza się przy dużej liczbie osób do przebadania. Tych wad pozbawione są kamery termowizyjne, pojawiające się już np. przy wejściach do szpitalnych SOR-ów.

Kamera Hikvision serii DS-2TD2636B umożliwia jednocześnie badanie do 30 osób, automatycznie wyszukując na obrazie twarze i mierząc temperaturę każdej z nich w obszarze jej zasięgu. Wyniki pomiarów z dokładnością $\pm 0,3^{\circ}\text{C}$ są wyświetlane w czasie rzeczywistym, indywidualnie dla każdej osoby. Kamera jednocześnie realizuje detekcję twarzy, wykonuje pomiar i generuje alarm w przypadku przekroczenia zadanej wartości temperatury. Opcjonalnie system można wzbogacić o rejestrator cyfrowy, który zapisze obraz wraz z danymi z pomiarów temperatury i umożliwi weryfikację, kto przebywał w pobliżu osoby z podwyższoną temperaturą.

Terminal pomiarowy z kontrolą dostępu...

Rozszerzeniem możliwości kamer termowizyjnych Hikvision są autonomiczne terminale pomiarowe Hikvision MinMoe, łączące funkcje monitora LCD, kamery termowizyjnej i kontrolera dostępu do pomieszczeń. Zależnie od modelu mogą być w wersji kompaktowej do montażu na ścianie bądź jako lekki przenośny stojak ustawiany np. przy wejściu czy w ciągach komunikacyjnych. Urządzenie wymaga jedynie podłączenia zasilania i opcjonalnie sieci komputerowej. Każda osoba pod-

chodząca do terminala widzi swoją twarz na ekranie, w tym czasie wykonywany jest pomiar temperatury, którego wynikiem jest komunikat głosowy i wizualny potwierdzający możliwość wejścia.

...i wykrywaniem maseczki w jednym

Terminal potrafi też wykryć, czy osoba nosi maseczkę. Zainstalowany przy drzwiach wejściowych, może je automatycznie zablokować, gdy badana osoba ma podwyższoną temperaturę lub nie nosi maseczki. Dostępna jest też funkcja szybkiego (poniżej 0,2 s) rozpoznawania twarzy na podstawie porównania obrazu z kamery z bazą danych obejmującą zdjęcia do 50 tys. osób. Zastosowane w terminalu algorytmy sztucznej inteligencji (AI) bezbłędnie rozpoznają osoby z bazy nawet w maseczkach. System automatycznie kontroluje dostęp do budynku, sprawdzając, czy osoba jest na liście uprawnionych do wejścia, ma maseczkę i przede wszystkim czy ma prawidłową temperaturę ciała.

Ile osób jest w obiekcie?

Do zliczania osób w danym obiekcie angażuje się teraz

pracownika ochrony, odciągając go od jego podstawowych obowiązków, nie ma też gwarancji, że nie popełni błędów w liczeniu. Automatyczne systemy liczące oparte na fotokomórkach montowanych najczęściej przy bramkach antykradzieżowych lub drzwiach nie są do końca precyzyjne. W dobie restrykcji sanitarnych i ściśle określonej liczby osób mogących jednocześnie przebywać w obiekcie taka sytuacja nie może mieć miejsca.

I tu znów z pomocą przychodzi AI. Kamera DS-2CD6825Go/C z dwoma obiektywami, umieszczona bezpośrednio nad wejściem, daje obraz stereoskopowy, który oprogramowanie kamery przekształca na model trójwymiarowy. Obiekty, które nie są osobami (np. zwierzęta, koszyki, wózki) nie będą liczone. Problemu nie stanowią osoby mijające się w polu pomiarowym czy wchodzące jednocześnie. Sztuczna inteligencja to potężne narzędzie do walki z pandemią, a przedstawione rozwiązania stanowią zaledwie część możliwości, jakie oferuje. Rozwiązania Hikvision do pomiaru temperatury zastosowano już w wielu obiektach handlowych (np. Galeria Aura Centrum w Olsztynie), w szpitalach (np. Szpital Specjalistyczny im. Stefana Żeromskiego SP ZOZ w Krakowie), biurach i na lotniskach.

Więcej informacji na stronie producenta: www.hikvision.com/europe/

Hikvision Poland

ul. Żwirki i Wigury 16B, 02-092 Warszawa
e-mail: info.pl@hikvision.com
<https://www.hikvision.com/europe/>





Autonomiczne układy kontroli dostępu i ich aktualizacja



W obecnych czasach zdalny dostęp do systemu jest normą. Ułatwienia polegające na zarządzaniu systemem kontroli dostępu z urządzeń mobilnych mają dać użytkownikowi elastyczność obsługi oraz pełną kontrolę zarządzania. Jednak im więcej sposobów dostępu do systemu, tym większa liczba potencjalnych „dziur”, które mogą być wykorzystane przez osoby niepowołane. Dlatego pomimo udogodnienia, jakim jest łącze zdalne, wiele firm nie decyduje się na umożliwienie dostępu przez tzw. sieć zewnętrzną. Rozwiązanie to znacznie ogranicza potencjalne możliwości interwencji osób niepowołanych oraz zapewnia stabilne działanie systemu.

Zamknięty układ, uniemożliwienie dostępu osobom nieupoważnionym i intruzom, brak złośliwego oprogramowania i konieczności aktualizacji systemu – czy na pewno są to same korzyści?

Praktyka często weryfikuje zagrożenia, które nie zawsze są widoczne na początku projektu. System kontroli dostępu (SKD) w jednym z biurów w Warszawie działał, korzystając tylko z własnej sieci zbudowanej na jego potrzeby. Serwer, który zarządzał wszystkimi kontrolerami systemu, był obsługiwany tylko przez dwie stacje robocze połączone fizycznie siecią wewnętrzną, a każdy operator miał indywidualne hasło. Program służący do zarządzania systemem działał szybko i ze stałą prędkością obliczeniową. W końcu była to autonomiczna sieć bez dostępu do środowiska zewnętrznego.

Rozwiązanie sprawdzało się przez lata, więc nie było potrzeby wprowadzania



T E K S T
Piotr Świderski

zmian. Jedyną możliwą modyfikacją była rozbudowa systemu w przypadku konieczności zwiększenia liczby przejść objętych kontrolą dostępu. Niestety właśnie fakt, że system funkcjonował tak długo bez większych problemów, miał po latach duże konsekwencje, które wpłynęły m.in. na ciągłość jego funkcjonowania. W myśl zasady, że skoro działa, nie należy nic zmieniać, inwestor nie odczuwał potrzeby modernizacji.

Pierwszą oznaką, że system KD zaczął pracować niepoprawnie, było to, że część danych była tracona (w tym przypadku użytkownicy biurowca posługiwali się kartami dostępu) – użytkownikowi przestawała działać karta dostępu. System został sprawdzony. Okazało się, że wpływ na awarię miał dysk twardej, który po ponad 5-letniej pracy zaczął tracić rekordy. Problem wydawał się błahy – dysk można wymienić, a system ma automatycznie robione *backupy*. Poprawność działania kontroli dostępu w budynku nie wydawała się zagrożona.

Rozwiązanie okazało się jednak nie tak łatwe, jak wydawało się na początku. Żyjemy w zmieniającym się świecie, powstają coraz nowsze technologie, chociaż na pewno są jeszcze fani starych rozwiązań, np. kaset VHS czy dysków CD. Każdy jednak zdaje sobie sprawę, że gdyby tego typu odtwarzacz stracił swoją użyteczność, jego naprawa albo wymiana byłaby w tym momencie nieopłacalna lub wręcz niemożliwa. Podobnie było w opisywanym przypadku. Okazało się, że nie można kupić nowego dysku, który byłby obsługiwany przez serwer systemu – serwer nie był już objęty wsparciem producenta i nie było możliwości wymiany dysków z kompatybilnością wsteczną. Skoro stary serwer nie mógł obsługiwać nowych dysków twardej, należało kupić nowy. A to wiązało się z kolejnymi wydatkami, np. na nowy *software*, na którym należało wgrać program do obsługi SKD. Jak można się domyślić, stary program do obsługi nie działał na nowym serwerze ze względu na brak dostępnych sterowników.

Po zakupie niezbędnych narzędzi okazało się, że dopiero teraz inwestor stanął przed największym wyzwaniem – przeniesienia danych (z całego kilkupiętrowego biurowca, wszystkich urządzeń plus użytkowników). Nowa wersja programu do obsługi systemu kontroli dostępu tak bardzo różniła się w zapisie danych, że nie było możliwości ich skopiowania i przeniesienia. Mimo zaangażowania dwóch firm i analiz technik zapadła decyzja – system będzie stawiany od nowa, a dane użytkow-

Aktualizacja wersji systemu nie wpływa bezpośrednio na jakość pracy, pozwala jednak znacznie ograniczyć koszty, które mogą pojawić się w razie awarii

ników muszą zostać przepisane „ręcznie”. Było to bardzo duże wyzwanie logistyczne w obiekcie, który funkcjonuje non stop, 24 godziny na dobę, 7 dni w tygodniu, z różnymi firmami.

Podsumowując, system kontroli dostępu w budynku był autonomiczny i działał świetnie. Jednak z powodu nieprzeprowadzenia aktualizacji doszło do dużego ryzyka, że przestanie działać i nie będzie możliwości jego naprawy w krótkim terminie. To z kolei doprowadziło do wygenerowania wysokich kosztów, na które złożyły się jednorazowy zakup pokaźnej dużej liczby sprzętu oraz duże nakłady pracy techników i innych osób zaangażowanych w projekt. Dlatego tak ważne jest posiadanie aktualnych wersji elementów systemu, a przynajmniej takich, które są stale wspierane przez producentów.

Mimo że aktualizacja wersji bezpośrednio nie wpływa na jakość pracy systemu czy odczucia użytkowników, zapewnia przede wszystkim lepszą kontrolę nad ciągłością działania systemu i pozwala znacznie ograniczyć koszty, które mogą się pojawić w razie awarii. ▣

B I O

Piotr Świderski

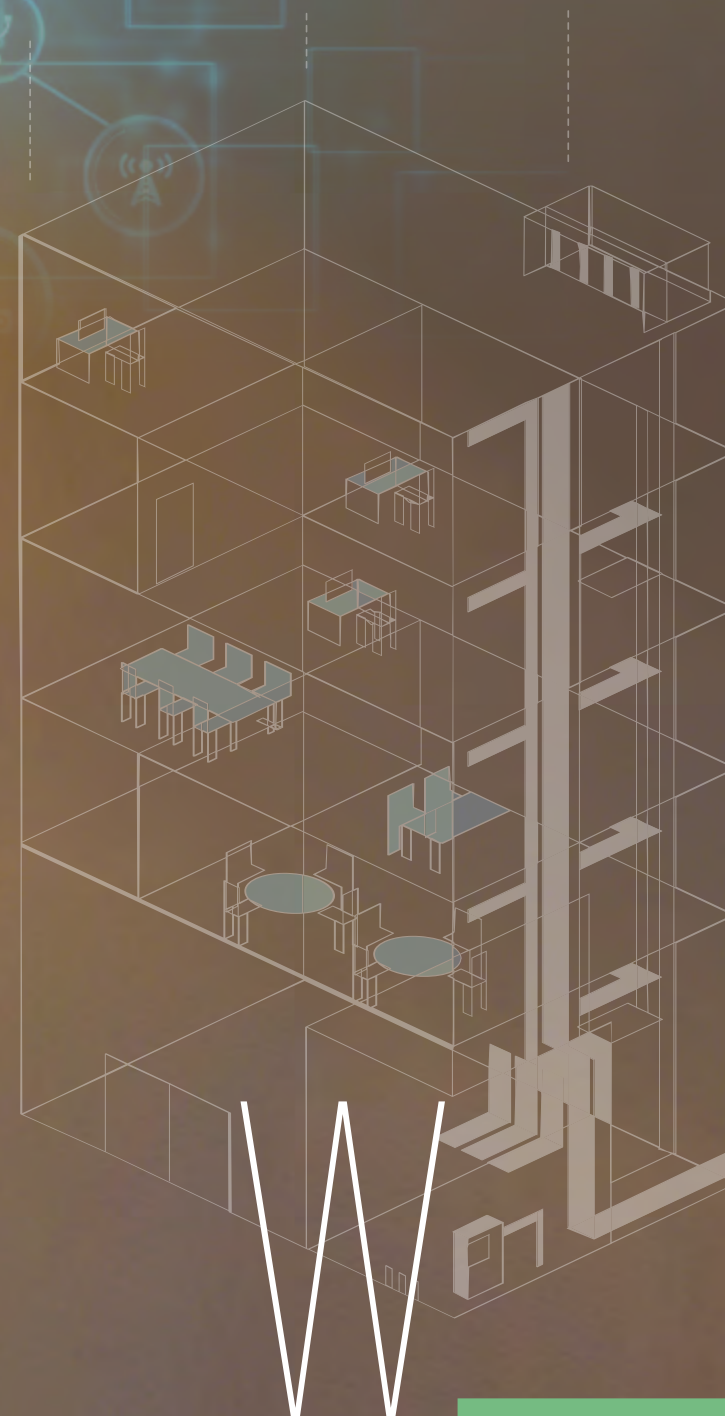
Absolwent PW Wydział Mechatroniki (mgr inż.). Ponad 8 lat doświadczenia w sektorze bankowym w departamentach bezpieczeństwa. Obecnie starszy specjalista ds. bezpieczeństwa w PwC.



WYZWAŃ ZWIĄZANYCH Z REALIZACJĄ KONTROLI DOSTĘPU W BIUROWCACH JEST WIELE, NP. NOWE MOŻLIWOŚCI SOFTWARE'OWE WYNIKAJĄCE Z PRZETWARZANIA W CHMURZE, PROBLEMY ZWIĄZANE Z DOBOREM ODPWIEDNICH PRZEWODÓW, CORAZ WYRAŹNIEJSZE TENDENCJE DO INTEGROWANIA SYSTEMÓW KONTROLI DOSTĘPU Z INNYMI SYSTEMAMI INSTALOWANYMI W BUDYNKU.

Systemy KD w biurowcach

O KONIECZNOŚCI KOORDYNACJI PRAC PROJEKTOWYCH



W artykule poruszam dwa tematy. Jeden jest związany z doбором armatury drzwiowej dla przejścia objętego kontrolą dostępu (KD), drugi dotyczy kwestii integracji systemu kontroli dostępu z systemem windowym. Wyboru dokonałem na podstawie własnych doświadczeń jako inżynier uruchomieniowy. W ostatnich latach te realizacje nastręczały najwięcej problemów, ich rozwiązywanie osobom uruchamiającym KD zajmowało dużo czasu, a problemy techniczne wynikłe w trakcie uruchomienia były najtrudniejsze do rozwiązania.



T E K S T

Michał Zalewski

W artykule projektantem będę nazywał generalnego projektanta, a inżynierem – inżyniera projektującego system kontroli dostępu (choć obaj są inżynierami i projektantami).

Armatura drzwiowa

Wydawałoby się, że to temat banalny. Dostawcy komponentów drzwiowych, takich jak sztaby magnetyczne, rygle, zamki elektromechaniczne, czujniki położenia rygla czy kontaktrony, mają ogromną ofertę najróżniejszych urządzeń. Problem ich wyboru jest traktowany jako poboczny – projektanci odpowiadający za kompleksowe zaprojektowanie budynku, łącznie z instalacjami, często tak właśnie podchodzą do niego.

Najczęściej obserwowaną praktyką jest wskazanie przez projektanta drzwi w biurowcu, które mają być objęte kontrolą dostępu. Zaprojektowanie systemu KD powierza się inżynierowi specjalistcie. Dostaje on plany budynku z wyznaczonymi drzwiami, które musi wyposażać w urządzenia kontroli dostępu. Będzie miał szczęście, jeżeli otrzymane wytyczne będą określały, jaka ma być kontrola: dwustronna czy jednostronna. Załóżmy, że lokalizacja drzwi przebiegała prawidłowo. Wystarczy, że inżynier rozmieści czytniki, przewidzi i opisze urządzenia wykonawcze i... udało się.

Zaraz, zaraz, nie tak szybko. Przecież projektant nie uzgodnił wyglądu czytników, ich rozmieszczenia w poszczególnych lokalizacjach względem framugi, włączników oświetlenia itp., bez tego projektu nie można zamykać. To są ważne aspekty, budynek musi wyglądać estetycznie. A skoro można dobrać prostokątne czytniki zamiast owalnych (bo bardziej pasują do marmurowych korytarzy), to dajmy taką możliwość projektantowi, bo i tak się o to upomni. I będzie miał rację, to też trzeba uzgodnić. Ale zwracam uwagę na „to też” w ostatnim zdaniu. Co jeszcze wymaga przeanalizowania? Wspomniana armatura drzwiowa. Nie jest możliwe, by inżynier projektujący system kontroli dostępu samodzielnie, bez niczyjej pomocy dokonał prawidłowych wyborów.

Drzwi mają wiele cech, które warunkują zastosowanie konkretnych komponentów, zaczynając od ich konstrukcji (jedno- czy dwuskrzydłowe, ze skrzydłem biernym), ciężaru i rodzaju materiału, z którego są wykonane, kończąc na możliwych do stosowania opcjach wyposażenia pozwalających np. na prowadzenie przewodów we framugach lub skrzydłach. Kolejnym aspektem są funkcje techniczne, jakie w obiekcie spełniają różne drzwi. Przy-



kładowo drzwi ewakuacyjne wyposażone w listwy przeciwpaniczne muszą mieć odpowiednią odporność ogniową. Zdarza się, że drzwi pełnią funkcję szczelnej przegrody ogniowej, otworu kompensacyjnego w systemach oddymiania lub np. czasowo muszą być otwarte na stałe (m.in. w archiwach lub strefach dostaw).

Mając świadomość tych cech, projektant musi zaplanować odpowiednie wyposażenie drzwi i uwzględnić je w projekcie w formie szczegółowych wytycznych w tzw. *doorliście* (specyfikacji). To jedyna gwarancja, że np. drzwi przeciwpożarowe, które dotrą na budowę, będą fabrycznie (przez producenta) właściwie przystosowane do pełnionej funkcji. Oczywiście niezbędna jest tu współpraca z inżynierem odpowiedzialnym za projekt kontroli dostępu. Koordynacja prac projektanta i inżyniera nie może ograniczać się tylko do potwierdzenia, że pracują na tej samej wersji planów budynku. Dobór odpowiedniej armatury drzwiowej jest zagadnieniem na styku dwóch branż: architektury i kontroli dostępu i tylko wspólna praca projektanta i inżyniera, zakończona podpisaniem karty koordynacji, daje szansę, że instalacje budynkowe będą działały prawidłowo.

Integracja systemu KD z systemem sterowania windami

To temat w zasadzie podobny, projektant słusznie zaplanował, by system kontroli dostępu był zintegrowany z systemem sterowania windami. Zapis pojawił się w dokumentacji, dostawca wind potwierdził, że sterownik jest przystosowany do integracji. Pełne zadowolenie. Pada pytanie o kształt czytnika, czy ma być owalny? Nie! Winda jest wyposażona w śliczny wyświetlacz ciekłokrystaliczny, wszystkie ściany są w lustrach, nie ma miejsca na czytnik. Najlepiej, żeby był schowany w obudowie windy, za panelem. Ale przecież obudowa panelu jest metalowa. W czym to przeszkadza? Ktoś zapewne nie uważał na lekcji fizyki na temat klatki Faradaya, ale nie wierzę, by nie zauważył, że telefon komórkowy przestaje w windzie działać...

Integracja systemu sterowania windy z systemem KD jest dużym wyzwaniem. Należy zacząć od precyzyjnego określenia dwóch wzajemnie wpływających na siebie funkcji: sprawnej, szybkiej windy oraz ograniczeń w dostępie dla osób nieuprawnionych. Prostszy przypadek – integracja wind w niewysokich budynkach, czyli funkcja hotelowa. Pasażer windy na poziomy recepcji i restauracji wjeżdża zawsze, na inne poziomy tylko za pomocą karty, którą przykład do czytnika w kabinie windy. Żeby tę funkcjonalność osiągnąć, należy wyposażyć windę w kabel zwirowy LAN, ustalić lokalizację czytnika w kabinie oraz zapewnić w sterowniku windy tyle wejść, ile jest „zastrzeżonych” pięter. W systemie kontroli dostępu należy przewidzieć taką samą liczbę wyjść. To są problemy na styku dwóch różnych instalacji i precyzyjne uzgodnienie zakończone podpisaniem karty koordynacji jest jedyną gwarancją, że integracja będzie działała prawidłowo.

O wiele trudniej jest w przypadku budynków wysokich (wielopiętrowych), tutaj integracja musi być realizowana programowo. Dwoch dostawców urzą-



Inżynier odpowiedzialny za projekt KD nie powinien podejmować samodzielnych decyzji bez koordynacji i uzgodnień merytorycznych z projektantem generalnym

dzeń (sterownika windy i systemu kontroli dostępu) musi uzgodnić typ portu komunikacyjnego, a także szczegółowy opis protokołu komunikacyjnego – ten opis protokołu jest wspomnianym wyżej stykiem pomiędzy dwiema instalacjami. Musi zostać uzgodniony i wspólnie podpisany. Tylko wtedy mamy pewność, że integracja będzie prawidłowa.

Trzeci, najtrudniejszy przypadek dotyczy systemu wind „inteligentnych”. Nie lubię tego słowa w odniesieniu do urządzeń, ale jest to dość powszechne. Producenci wind do budynków wyposażonych w wiele wind obsługujących dużą liczbę pięter z dużą liczbą pasażerów coraz częściej wyposażają budynki w systemy komputerowe zliczające osoby, dobierające odpowiednio trasę wind do liczby zgłoszeń na piętrach, pozwalające np. przygotować się do obsługi porannej poprzez natychmiastowy zjazd wind na określony poziom itd.

W tym przypadku integracja z KD jest najbardziej skomplikowana. Wymaga pełnego zintegrowania baz danych systemu wind z bazą systemu kontroli dostępu. To zadanie najtrudniejsze, gdyż angażuje programistów po obu stronach. Ponadto wymaga pisemnego potwierdzenia zgodności programowej przez obu producentów. Są dostawcy wind, którzy podejmują temat, badają wspólnie z dostawcami kontroli dostępu interfejs i wydają certyfikaty zgodności.

Temat ten trzeba dokładnie analizować na etapie wyboru dostawców wind oraz systemu kontroli dostępu. Może się okazać, że wybierając określonego dostawcę wind, zawężamy możliwości wyboru

systemu kontroli dostępu. Wybór dostawców, którzy mają gotowe oprogramowanie integracyjne, ułatwi uruchomienie. Brak gotowych rozwiązań może wręcz zablokować możliwości integracji.

Często dostawcy wind oferują własne czytniki kart wpięte do ich systemu windowego i niechętnie podejmują się zintegrowania systemu bez dostawy tych elementów. Nastręcza to jednak ogromne trudności eksploatacyjne. Jeżeli użytkownik pozwoli na utworzenie niezintegrowanych baz danych użytkowników: jednej w systemie windowym, drugiej w systemie kontroli dostępu, będzie musiał zdublować pracę administracyjną związaną z rejestracją użytkowników oraz nadawaniem i kasowaniem uprawnień. I to pod warunkiem że systemy będą pracowały w oparciu o ten sam typ karty. Trzeba o tym pamiętać przy planowaniu tych systemów.

Podsumowując, temat nie jest prosty. Podjęcie się zarówno jednego, jak i drugiego zadania samodzielnie przez inżyniera kontroli dostępu, bez wsparcia ze strony projektanta generalnego i dostawcy wind na odpowiednio wczesnym etapie, może mieć ogromne konsekwencje dla sprawnego uruchomienia systemów.

B I O

mgr. inż. Michał Zalewski

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 24 lat, od 12 lat niezależny konsultant, inżynier uruchomieniowy.

Uwagi końcowe

Nasuwa się pytanie, dlaczego ten temat został podjęty w czasopiśmie branżowym skierowanym m.in. do inżynierów teletechników, a nie w piśmie dla projektantów lub dostawców wind. Jako inżynier uruchomieniowy z wieloletnim doświadczeniem chciałem uświadomić kolegom teletechnikom, że mają prawo wymagać od specjalistów z innych dziedzin wsparcia technicznego przy planowaniu takich zadań. Nie powinni podejmować samodzielnie decyzji bez koordynacji i uzgodnień merytorycznych ze styku różnych branż. Nie dlatego, że nie potrafią, mogą po prostu nie znać pewnych aspektów związanych z projektem.

Jeżeli zmuszeni przez okoliczności projektowe podejmują się rozwiązania tych problemów i trafiają na trudności, to nie jest ich wina. Rozwiązując je samodzielnie, bez wsparcia, niepotrzebnie zdejmują z innych odpowiedzialność, która z założenia jest wspólna, tak jak wspólnie jest zadanie.

Tylko współpraca specjalistów z różnych dziedzin gwarantuje sukces uruchomieniowy

Często w końcowej fazie realizacji jestem zmuszony odpowiadać na pytania, dlaczego coś nie działa, jak można problem rozwiązać, kto powinien to zrobić, czego brakuje w systemach lub wyposażeniu. I najczęściej muszę odpowiadać: ponieważ nie było odpowiedniej koordynacji prac, wyboru urządzeń bądź wyposażenia dokonano bez uwzględnienia kompletu uwarunkowań, że wyposażenie fizyczne lub programowe urządzeń nie zostało uzgodnione albo rozwiązania zastosowane dla osiągnięcia jednego celu technicznego uniemożliwiają realizację innych funkcji (np. sztaba magnetyczna zainstalowana w świetle drzwi obniża prześwit).

Wiem, że nie odpowiedziałem na wiele pytań, nie dałem gotowych recept – nie to było moją intencją. Chciałem temat poruszyć, byśmy (inżynierowie teletechnicy) głośno i odważnie potrafili mówić: nie powinno się używać słów „tylko” czy „wystarczy”, bo to wróży problemy z uruchomieniami. ▣

DETEKCJA CZŁOWIEKA
Eliminacja fałszywych alarmów w monitoringu

ZLICZANIE LUDZI W STREFIE
Dokładne zliczanie ludzi w strefach handlowych i transporcie

ANALITYKA I SYSTEMY LPR/LPC
Wysokiej jakości inteligentny monitoring wideo

PANORAMICZNE KAMERY
Wydajne systemy panoramiczne 180°/360°

LICZENIE LUDZI I POJAZDÓW
Systemy liczenia dużej dokładności 3D i 2D

VIVOTEK

Dystrybucja • Projekty • Integracja • Współpraca

SUMA.COM.PL



RYNEK SECURITY



SATEL KNX - automatyka budynkowa na najwyższym poziomie

KNX jest jednym z najczęściej stosowanych na świecie uniwersalnym systemem automatyki budynkowej. Standard ten jest stale rozwijany, tak jak i Stowarzyszenie KNX zrzeszające producentów zaawansowanej elektroniki z całego świata, każdego roku przyjmujące nowych członków. Firma SATEL nie tylko należy do tego elitarnego grona liczącego prawie 500 podmiotów, ale także z początkiem 2020 r. wprowadziła do swojej oferty nową grupę produktów zgodną z tym międzynarodowym standardem: moduły SATEL KNX.



Prezentujemy 8 nowości, które od szkicu po gotowy produkt powstały w firmie SATEL. Są to: urządzenia wykonawcze (tzw. aktry), moduł wejść binarnych (tzw. sensor), interfejs do programowania systemu oraz zasilacz magistrali KNX.

Wygodnie steruj oświetleniem

Listę otwiera KNX-DIM21 – uniwersalny aktor ściemniający, przeznaczony do płynnego sterowania źródłami światła zasilanymi z sieci 230 V AC lub przez transformator. Na każdym z dwóch kanałów mogą pracować odbiorniki o mocy do 300 W. Typ podłączonego obciążenia (R, L, C) jest automatycznie wykrywany, a moduł dopasowuje charakterystykę sterowania.

Przesuń, podnieś, rozwiń

Modele dwukanałowych aktorów żaluzyjnych KNX-BSA12L i KNX-BSA12H służą do precyzyjnego sterowania położeniem różnego rodzaju zasłon (żaluzji poziomych i pionowych, rolet, markiz), karniszy czy okien. KNX-BSA12L przeznaczony jest do urządzeń zasilanych napięciem 24 VDC, nato-

miast KNX-BSA12H znajdzie zastosowanie przy napędach 230 VAC.

Włączaj i wyłączaj

Kolejną parę tworzą uniwersalne aktry KNX-SA41 oraz KNX-SA24. Umożliwiają przełączanie stanu różnych urządzeń, np. oświetlenia, wentylatorów, napędów bram czy elektrozasłorów. Pierwszy z modułów ma cztery niezależne tory, po jednym przekątniku (kanale) na tor, drugi zaś – dwa niezależne tory z czterema kanałami każdy. Dzięki temu można np. sterować urządzeniami zasilanymi z różnych faz.

Szerokie możliwości

KNX-BIN24 to uniwersalny moduł wejść binarnych. Odbiera zarówno telegramy od urządzeń magistrali KNX, jak i sygnały cyfrowe spoza niej, np. od przycisków, włączników, styków kontaktronów. Między jego ośmioma kanałami odbiorczymi można tworzyć relacje logiczne i czasowe. Moduł ma 20 bloków funkcyjnych pobudzanych z kanałów wejściowych, którym można przypisać różne funkcje sterujące. Sygnały wejściowe oraz wyjściowe z bloków funk-

cyjnych mogą być ponownie/wielokrotnie użyte w innych blokach.

Stabilne zasilanie to podstawa

Zasilacz KNX-PS640 montowany na szynie DIN służy do zasilania magistrali KNX napięciem systemowym (SELV) 28...30 VDC. Maksymalny prąd wyjściowy wynosi 640 mA. Do zalet zasilacza należy wysoka odporność na zwarcia (na wejściu i na wyjściu) oraz na przeciążenia.

Programowanie i zapis danych

Do połączenia magistrali i komputera, na którym zainstalowany jest program konfiguracyjny ETS, można wykorzystać interfejs KNX-USB. Jego atutem jest możliwość pracy w trybie logowania magistrali – historia zdarzeń (ruch telegramów) jest zapisywana w pamięci nieulotnej, a dane można wyeksportować do plików CSV lub XML. Niewielkie rozmiary, mobilność i możliwość zasilania z powerbanku sprawiają, że interfejs można zabrać do torby za laptopem, a następnie w obiekcie podłączyć go na kilka dni do instalacji w celu weryfikacji poprawności jej działania i diagnozowania błędów.

Wyjątkową cechą rozwiązań SATEL jest możliwość łatwej integracji – inteligentną instalację KNX można powiązać z systemem sygnalizacji włamania i napadu INTEGRA za pośrednictwem modułu INT-KNX-2. Dzięki temu sygnały z systemu SSWiN można wykorzystać w systemie KNX, i na odwrót. W efekcie użytkownicy będą mogli za pomocą jednego manipulatora (np. dotykowego INT-TSI) lub aplikacji mobilnej INTEGRA CONTROL sterować funkcjami systemu alarmowego i automatyki budynkowej KNX.

SATEL

ul. Budowlanych 66
80-298 Gdańsk
www.satel.pl



INTELIGENTNY BUDYNEK Z SATEL KNX – SZEROKIE MOŻLIWOŚCI

- ✓ Realizacja scen i skomplikowanych scenariuszy łączących pracę różnych urządzeń
- ✓ Elastyczna rozbudowa i modyfikacja systemu
- ✓ Integracja z zaawansowanym systemem alarmowym INTEGRA

www.satel.pl

BEZPIECZNE SZPITALE z rozwiązaniami security

Zdalny pomiar temperatury

Pandemia SARS-CoV-2 jeszcze silniej wyeksponowała problemy, z jakimi od lat boryka się polska służba zdrowia. Instytut Zdrowia Publicznego CM UJ przy współpracy z Open Eyes Economy przygotował raport „Szpitale w czasie pandemii i po jej zakończeniu”, w którym obnażył największe bolączki systemu ochrony zdrowia.



Głównymi problemami, na jakie zwrócono uwagę, są m.in. chaos organizacyjny, braki kadrowe czy trudna sytuacja finansowa. Do propozycji najważniejszych działań w związku z epidemią zaliczono zapewnienie bezpieczeństwa na „linii frontu”. Może w tym pomóc technika ochronna – urządzenia i systemy zabezpieczeń oferowane przez firmy branży security. Prezentujemy kilka przykładów wdrożeń wspomagających i ułatwiających pracę polskim szpitalom w surowym reżimie sanitarnym. Placówki medyczne są zobowiązane do przestrzegania restrykcyjnych wymogów bezpieczeństwa. Jedną z podstawowych praktyk mających na celu wykrycie potencjalnego zagrożenia – zakażenia koronawirusem i pierwszych symptomów choroby COVID-19 – jest kontrola temperatury ciała osób, które muszą przekroczyć szpitalne progi. Wyzwaniem dla wielu placówek było sprawne zorganizowanie pomiarów zarówno wśród pacjentów, jak i personelu medycznego.

MACIEJ PIETRZAK, Dahua Technology Poland

– Opracowany przez naszą firmę system zdalnego pomiaru temperatury ludzkiego ciała został zainstalowany już w kilku placówkach medycznych w Polsce. Skuteczność i przede wszystkim dokładność pomiaru, jakimi system wyróżnia się na tle innych dostępnych na rynku rozwiązań, wynika z wykorzystania kamery termowizyjnej o wysokiej czułości w połączeniu ze wzornikiem – black body, który odgrywa tu kluczową rolę. Zastosowane w kamerze algorytmy AI pozwalają na precyzyjny pomiar w określonych punktach, np. kąciku oka. Muszę podkreślić, że rzeczywista dokładność pomiaru wynosi $\pm 0,3^{\circ}\text{C}$. Wszystko to sprawiło, że nasze rozwiązanie zyskało zaufanie szpitali – miejsc, gdzie pacjenci i personel są szczególnie narażeni na infekcję.

dr ELŻBIETA KASPRZAK, prezes Zarządu Szpitala Miejskiego im. Jana Garduły w Świnoujściu

– Do tej pory personel medyczny mierzył temperaturę ręcznym termometrem przed wejściem do budynku. Niekwestionowaną wadą takiego rozwiązania był fakt, że odbywało się to w bezpośrednim kontakcie z odwiedzającymi naszą placówkę. Ponieważ każda osoba musi być sprawdzona, prowadziło to czasami do sytuacji, że kilka osób musiało czekać na pomiar w niewielkim przedśionku, co zwiększało ryzyko zakażenia. System automatycznie mierzący temperaturę ciała przy wykorzystaniu kamery termowizyjnej Dahua Technology znacząco usprawnił działanie naszego szpitala. Ruch odbywa się teraz płynnie, ale przede wszystkim poprawiliśmy komfort i bezpieczeństwo zarówno naszych pacjentów, jak i personelu medycznego.

STANISŁAW SOWA, dyrektor Oddziału Zachód Fire-Max

– SEEK SCAN to jedno z najbardziej przystępnych cenowo rozwiązań obrazowania termicznego, które pozwala na zautomatyzowany pomiar temperatury ciała z zachowaniem bezpiecznej odległości. SEEK SCAN w ciągu kilku sekund automatycznie skanuje twarz, dokonuje pomiaru temperatury z dokładnością do $\pm 0,3^{\circ}\text{C}$ i uruchamia alarm wizualny oraz dźwiękowy w przypadku wykrycia osoby z gorączką. System może być uruchomiony w kilka minut bez specjalnego szkolenia. SEEK SCAN spełnia wytyczne FDA dotyczące wstępnej oceny temperatury ciała podczas COVID-19 Public Health Emergency. Różnorodność zalet i niewysoka cena tego systemu była podstawowym atutem przy zakupie przez poznański szpital. Obecnie tym systemem zainteresowało się wiele innych szpitali w Polsce.

– Rozwiązanie pozwala na dokonanie wstępnej oceny stanu zdrowia pacjentów, znacząco usprawniając cały proces oraz minimalizując ryzyko bezpośredniego kontaktu z osobą potencjalnie zarażoną COVID-19. Systemy zostały zainstalowane w naszym Centrum Technologicznie Wspomaganej Rehabilitacji. Są tu przyjmowani na turnusy rehabilitacyjne pacjenci cierpiący na dziecięce porażenie mózgowe. Zastosowanie systemu zautomatyzowanego pozwala wyeliminować u tych pacjentów stres związany z pomiarem temperatury przez nieznaną im osobę, na której byłoby narażenie podczas stosowania klasycznych termometrów. Muszę podkreślić, że pomiar jest szybki, pozwala zminimalizować opóźnienia wykonywania świadczeń

**dr n. med. PRZEMYSŁAW
DAROSZEWSKI,
Dyrektor Ortopedyczno-
-Rehabilitacyjnego Szpitala
Klinicznego im. Wiktora Degi
Uniwersytetu Medycznego
im. Karola Marcinkowskiego
w Poznaniu**

– Firma Hikvision może pochwalić się wieloma wdrożeniami. Nasze rozwiązania eliminują problemy zachowania odpowiedniego dystansu pomiędzy osobą mierzącą temperaturę pacjenta tradycyjnym termometrem a pacjentem mogącym być potencjalnym nosicielem koronawirusa wywołującego COVID-19. Kamera termowizyjna z rejestratorem stanowi kompletny system odpowiadający potrzebom użytkownika. Na szczególną uwagę zasługuje wysoka dokładność pomiaru, wynosząca $\pm 0,5^{\circ}\text{C}$ przy zastosowaniu kamer bez zewnętrznego źródła referencyjnego (tzw. blackbody). We współpracy ze wzornikiem blackbody kamery mierzą z dokładnością nawet $\pm 0,3^{\circ}\text{C}$. Zastosowanie algorytmów sztucznej inteligencji w wybranych modelach pozwala na automatyczne wykrywanie twarzy w grupie osób i jednoczesny, błyskawiczny pomiar temperatury wielu osób. Nasze systemy działają już w wielu miejscach, z czego się bardzo cieszymy

**PIOTR ŚWIDER,
Business Development
Manager
Hikvision Poland**

**lek. med.
ŁUKASZ LITWA,
kierujący oddziałem
ratunkowym w Szpitalu
Specjalistycznym
im. Stefana Żeromskiego
SP ZOZ w Krakowie**

– Zainstalowana kamera mierzy temperaturę ciała szybko, łatwo, a przede wszystkim w sposób bezinwazyjny. System pozwolił na sprawną ocenę wszystkich pacjentów Szpitalnego Oddziału Ratunkowego. Kamera jest niezaprzeczalnie w sytuacji epidemii, obecnie jest wykorzystywana do pomiaru temperatury pracowników szpitala przychodzących do pracy. Daje to nam szansę na ograniczenie ryzyka transmisji potencjalnego zakażenia wśród personelu i pacjentów szpitala. System w swojej autonomii właściwie nie wymaga ciągłej obserwacji obrazu – uruchamiany automatycznie alarm ogranicza interwencje pracowników SOR do minimum. Nie mogą też pominąć psychologicznego wpływu na pacjentów i pracowników szpitala, którzy czują, że są otoczeni opieką już od momentu przekroczenia progu SOR. Urządzenia są estetyczne i kompaktowe, co pozwoliło na zainstalowanie rejestratora i monitora w niewielkiej recepcji. System jest praktycznie bezobsługowy.

* <https://cowzdrowiu.pl/aktualnosci/post/szpital-w-czasie-pandemii-problemy-oraz-rekomendacje-na-przyszlosc>



BEZPIECZNE
SZPITALE



JAKUB SOBEK, Linc Polska

– Szybko, łatwo, a przy tym bardzo skutecznie. Te słowa najlepiej charakteryzują rozwiązanie Kentix SmartXcan. Urządzenie może działać niezależnie, można je też zintegrować np. z automatycznymi drzwiami, bramkami, blokując wstęp osobom z gorączką. Czerwona dioda na interfejsie automatycznie informuje o podwyższonej temperaturze ciała, zielona oznacza, że jest ona w normie. Ponad 1000 punktów pomiarowych oraz algorytmy sztucznej inteligencji gwarantują uzyskiwanie dokładnych, odpornych na manipulację wyników. Dodatkowo urządzenie można wyposażać w czytnik RFID, który pozwoli na identyfikację pracownika, kontrolowany dostęp oraz ewidencję czasu wejść i wyjść z obiektu.

To idealne połączenie funkcjonalności bezdotykowego pomiaru temperatury ciała z rozwiązaniem do kontroli dostępu. Dzięki temu pomiar temperatury staje się rutynową czynnością przy każdym wejściu do budynku. Podjęcie takich długofalowych działań będzie miało pozytywny wpływ na bezpieczeństwo nas wszystkich.



– Po ogłoszeniu stanu epidemicznego zaistniała konieczność pomiaru temperatury wszystkich pracowników wchodzących do szpitala. Uniwersytecki Szpital Dziecięcy w Krakowie poszukiwał systemu prostego w konfiguracji i łatwego w użytkowaniu. Przetestowaliśmy kilka rozwiązań i w końcu trafiliśmy na system Kentix, który najlepiej spełnia nasze potrzeby – szybki, bezobsługowy pomiar temperatury pracowników wchodzących do budynku. Okazał się też perspektywiczny, daje nam możliwość rozbudowy o kolejne moduły i integrację z kontrolą dostępu. Po kilku dniach użytkowania wszyscy pracownicy sprawnie przechodzą cały proces kontroli, a wejście do szpitala zajmuje kilka sekund.

KATARZYNA CIEMNY, kierownik Działu Aparatury Naukowo-Medycznej Uniwersytecki Szpital Dziecięcy w Krakowie



MICHAŁ NOCÓŃ, dyrektor działu handlowego Promitel

– Wiedząc, jakie korzyści przynoszą nowoczesne systemy, oczywiste było dla nas, że każdy szpital powinien z nich korzystać. Kamery z dużą dokładnością mogą dokonać pomiaru temperatury nawet 30 osobom równocześnie. Tradycyjnym termometrem można w tym samym czasie zbadać tylko jedną osobę.

Nasz dział techniczny przetestował wszystkie modele kamer do pomiaru temperatury i jesteśmy pewni, że system zainstalowany w Górnośląskim Centrum Zdrowia Dziecka przyczyni się do zapewnienia bezpieczeństwa i ułatwi pracę w tym trudnym okresie.



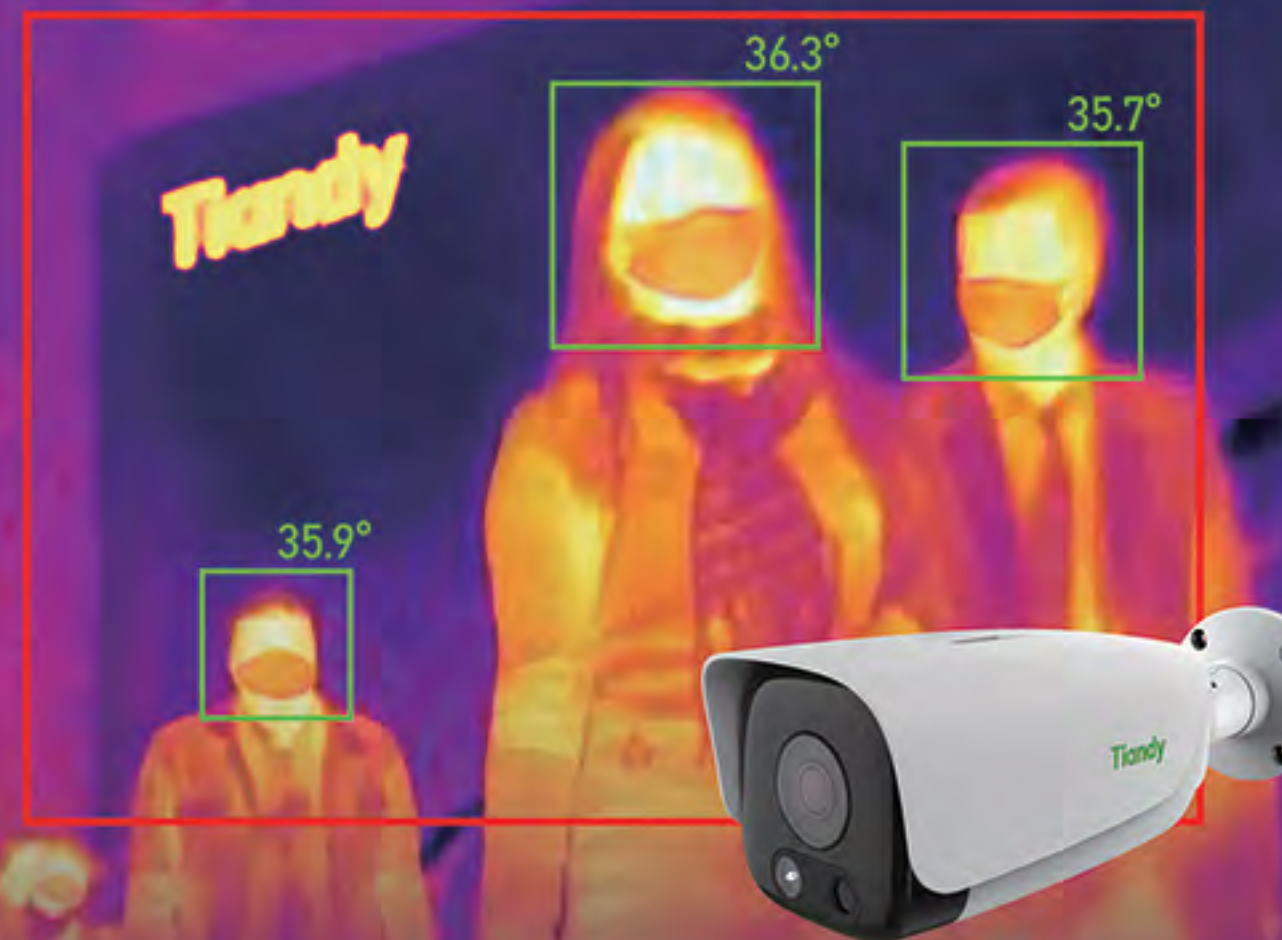
WOJCIECH GUMUŁKA, rzecznik prasowy Górnośląskie Centrum Zdrowia Dziecka w Katowicach

– Dziękujemy firmie Promitel, która przekazała na rzecz naszego szpitala system automatycznego pomiaru temperatury ciała. Sprawdzając temperaturę, system ten zwiększa bezpieczeństwo leczonych u nas dzieci i naszego personelu.

Dzięki jego zastosowaniu otrzymaliśmy zabezpieczenie, które nie wymaga od nas dodatkowego zaangażowania, a jednocześnie skutecznie chroni szpital przed rozprzestrzenianiem się wirusa, wykrywając podwyższoną temperaturę, będącą głównym symptomem zakażenia. □

Tiandy

Genway



KAMERA TERMOWIZYJNA Z POMIAREM TEMPERATURY CIAŁA TO JEST TIANDY

TC-C34LP Spec: I5/E/T/4mm 0.0002Lux@F1.0



Genway oficjalny Dystrybutor Tiandy

Email: info@genway.pl

Tel: +48-24-264-77-33

Strona: www.genway.pl

Fax: +48-24-268-12-29



BEZPIECZNE
SZPITALE

Standardy bezpieczeństwa w pomieszczeniach sterylnych, szpitalach, laboratoriach, zakładach produkcyjnych przemysłu farmaceutycznego są niezwykle wysokie i podlegają surowym wymaganiom technicznym. Zasady bezpieczeństwa są nadrzędne, ale często utrudniają komunikację na stanowisku pracy.

Bezpieczna komunikacja w sterylnych warunkach

Zaawansowany technicznie system komunikacji Commend płynnie integruje się z wymagającymi środowiskami pracy, przyczyniając się do zwiększenia wydajności przy jednoczesnej poprawie bezpieczeństwa pracy. To higieniczne rozwiązanie zaprojektowano zgodnie z GMP (Good Manufacturing Practice), posiada też Atest Higieniczny wydany przez PZH.

Podstawowym zadaniem rozwiązań interkomowych Commend jest zapewnienie łączności głosowej pomiędzy strategicznymi miejscami szpitala czy innymi wymagającymi sterylności pomieszczeniami. Umożliwiają to terminale firmy Commend instalowane w salach chorych, salach operacyjnych, pomieszczeniach personelu, laboratoriach, przejściach, windach i innych pomieszczeniach użytkowych. Personel medyczny może komunikować się między sobą, a także z centralnymi i pomocniczymi punktami systemu. Rolę tych drugich odgrywają zwykle dyżurki pielęgniarskie. Centralne punkty systemu najczęściej lokuje się w dyżurce szpitala. Stacje interkomowe mogą pełnić jednocześnie funkcję kontroli dostępu (sterowanie drzwiami). Pielęgniarka może z poziomu interkomu wpuścić interesantów na oddział, nie opuszczając stanowiska pracy.

Szpital Miejski w Świnoujściu wykorzystał takie rozwiązanie do komunikacji w salach operacyjnych, gabinetach lekarzy i pielęgniarek. Pulpity interkomowe znajdują się we wszystkich pomieszczeniach tzw. strefy czystej tej placówki.

– System łączności interkomowej firmy Commend zapewnia komunikację między głównym punktem pielęgniarskim, gabinetami zabiegowymi, salami operacyjnymi, pracownikami RTG. Stacje interkomowe posiadają wymagane certyfikaty i dopuszczenia jednostek zewnętrznych – mówi Leszek Schmidt, kierownik działu w C&C Partners.

Wyróżniającym się modelem stacji interkomowej jest WS800FMD, który posiada zgodność z normami EN14644-1 Kła-



sa 1-9 (klasyfikacja pomieszczeń czystych) oraz IEC60601-1 (norma EMC dla urządzeń medycznych). Co więcej, jest wyposażony w membranę uszczelniającą o działaniu antybakteryjnym. Oznacza to, że powierzchnia jest zabezpieczona przed namnażaniem się bakterii! Urządzenia zostały przetestowane w firmach farmaceutycznych i szpitalach przy użyciu środków dezynfekcyjnych i płynów do sterylizacji. W sytuacjach alarmowych bądź przy poszukiwaniu pracowników dużym ułatwieniem jest możliwość nadawania przez system Commend rozgłoszeń grupowych na interkomy, systemy rozgłoszeniowe PA, radiotelefony działające w określonym miejscu bądź w całym szpitalu.

Pacjent pod czujnym... uchem

Zastosowanie zintegrowanego systemu łączności znacznie też poprawia jakość opieki nad pacjentami. Można go integrować z dowol-

nym rozwiązaniem przyzywowym. W jego skład wchodzi cieżna lub przyciski przy łóżkach chorych, terminale przy łóżkach lub jeden na pokój, lampki sygnalizacyjne nad drzwiami wejściowymi do sali oraz przyciski kasowania, przywołania czy wezwania lekarza. W momencie aktywacji wezwania system wysyła informację o zdarzeniu na wskazane terminale (pielęgniarka).

Zarządzanie bezpieczeństwem z jednego miejsca

Operator centrum zarządzania systemu łączności może także korzystać z systemów zarządzania informacją o bezpieczeństwie fizycznym klasy PSIM+ integrujących systemy kontroli dostępu, sygnalizacji włamania i napadu, monitoringu wizyjnego oraz omawiany system interkomowy Commend. Umożliwia on zarządzanie wszystkimi elementami z poziomu wspólnego interfejsu użytkownika, który zapewnia odpowiednio wcześnie alarmowanie o stanach zagrożeń, archiwizację zdarzeń wraz ze skorelowanym zapisem wideo i podejmowanie stosownych działań, procedur czy odpowiednich polityk bezpieczeństwa w sytuacjach kryzysowych. □

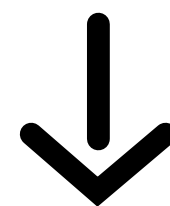
C&C Partners

ul. 17 Stycznia 119, 121,
64-100 Leszno
<https://www.ccpartners.pl>



www.aspolska.pl

Systemy sygnalizacji pożarowej w służbie zdrowia w czasach COVID-19



Obecnie w czasie pandemii COVID-19 sektor opieki zdrowotnej stał się być może najbardziej wrażliwą, wystawioną na ciężką próbę branżą. Ostatnią rzeczą, o którą placówki służby zdrowia powinny się teraz martwić, jest ich system sygnalizacji pożarowej.

W przypadku alarmu pożarowego i konieczności ewakuacji pacjentów niektórzy z nich mogą potrzebować pomocy. Ze względu na stosowanie respiratorów u chorych przebywających na oddziale intensywnej terapii i ryzyko rozprzestrzenienia się chorób zakaźnych, ewakuacja staje się niezwykle trudna, a czasem nawet niemożliwa.

Kluczowe jest zapobieganie fałszywym alarmom

Fałszywy alarm pożarowy jest groźny dla funkcjonowania każdej placówki służby zdrowia. Takie zdarzenie może prowadzić do przerw w świadczeniu usług i powodować pogorszenie się opieki nad pacjentami. Z tego powodu kluczowa staje się minimalizacja występowania takich zdarzeń. Badania* dotyczące alarmów pożarowych w placówkach służby zdrowia pokazują, że najczęstszą przyczyną fałszywych alarmów jest gotowanie. Kolejnymi na li-

ście są: prace konserwacyjne i serwisowe firm zewnętrznych, awarie elektryczne, pojawienie się pary wodnej, palenie papierosów w miejscach niedozwolonych, nieuprawnione uruchomienie ręcznych ostrzegaczy pożarowych i kurz.

Jak więc zapobiegać takim alarmom? Prace należy rozpocząć już na etapie projektowania systemu sygnalizacji pożarowej i dbać o tę kwestię przez cały cykl jego życia. Jednym ze skutecznych sposobów na ograniczenie liczby fałszywych alarmów jest zastosowanie czujek pożarowych wielosensorowych. Tryby ich pracy można odpowiednio dostosować do warunków w obiekcie, np. ustalając większą czułość albo większą odporność na takie czynniki, jak kurz czy para wodna.

Możliwość zaprogramowania różnych trybów pracy takiej czujki i różnych poziomów jej czułości, niezależnie dla trybu dziennego (z obsługą) i nocnego (bez obsługi), pozwala zmniejszyć liczbę fałszywych alarmów bez obniżania poziomu bezpieczeństwa.

Zastosowanie czujek wielosensorowych zwiększa też elastyczność systemu. Idealnie sprawdzają się one w budynkach, w których przeznaczenie różnych pomieszczeń może się często zmieniać (jak np. w czasie obecnej epidemii). W takim przypadku zawsze konieczna jest weryfikacja, czy model czujki zainstalowanej w danym obszarze jest wciąż odpowiedni do jak najszybszego wykrywania pożaru. Jeśli są to czujki wielosensorowe, prosta zmiana sposobu jej pracy najczęściej

w zupełności wystarcza, nie są wymagane żadne fizyczne zmiany w systemie (np. wymiana jednego modelu czujki na inny). Firma Zettler posiada doskonale rozwiązanie w postaci czujek wielosensorowych 30Tec®. Czujki serii 830PC oraz 850PC mają trzy sensory: dymu, ciepła i tlenku węgla, które mogą być skonfigurowane na wiele różnych sposobów (trybów) i poziomów czułości. Pozwala to w pełni wykorzystać wszystkie opisane powyżej sposoby radzenia sobie z fałszywymi alarmami.

Ratowanie życia zaczyna się od projektu SSP

Systemy sygnalizacji pożarowej w ośrodkach opieki zdrowotnej służą przede wszystkim ochronie życia, ale pełnią też ważną funkcję w ochronie mienia. Wczesne ostrzeżenie o pożarze minimalizuje również zakłócenia w funkcjonowaniu obiektu i zapewnia szybkie wznowienie obsługi pacjentów. Niezwykle więc ważne jest, aby już na wczesnym etapie ustalić wymagania projektowe i eksploatacyjne dla systemu sygnalizacji pożarowej. Muszą one uwzględniać ogólną strategię bezpieczeństwa pożarowego danego obiektu i jego szczególne procedury ewakuacyjne.

Aby uzyskać więcej informacji na temat projektowania i planowania systemów sygnalizacji pożarowej w obiektach służby zdrowia, odwiedź naszą stronę: www.zettlerfire.com □

Johnson Controls International

ul. Krakowiaków 50
02-255 Warszawa
pawel.jozwik@jci.com



*Źródło: raport HTM 05-03:L, w którym przedstawiono dane o zdarzeniach pożarowych zgłoszonych do Ministerstwa Zdrowia w Anglii w okresie od 1994/95 do 2004/05.



Wpływ pandemii koronawirusa na bezpieczeństwo w szpitalu

Pandemia COVID-19 wstrząsnęła światem i wygenerowała nowe wzorce zachowań i procedur we wszystkich gałęziach gospodarki, a także – co jest szczególnie ważne – w sektorze służby zdrowia. Kryzys z nią związany postawił też przed administracją rządową nowe, bardzo zróżnicowane wymagania i problemy, takie jak brakujące miejsca w placówkach szpitalnych, konieczność restrukturyzacji całych obiektów medycznych, przystosowywanie ich do nowych realiów opieki nad pacjentami w dobie masowych zakażeń poprzez wydzielenie stref bezpieczeństwa i oddziałów objętych kwarantanną.



Na całym świecie rozpoczęto w ekspresowym tempie budowę nowych szpitali zakaźnych, żeby zapewnić odciążenie nadwyrężonej służby zdrowia. Wprowadzono też specjalne procedury zachowania środków ostrożności w kontaktach z pacjentami pozostającymi w izolacji. Do tej pory, w warunkach normalnego funkcjonowania jednostek medycznych, kontakt osobisty personelu z pacjentami był nieodzownym elementem codziennej pracy. W dobie pandemii zmniejszenie bezpośredniego kontaktu pomiędzy osobami jest najlepszym rozwiązaniem, które może zredukować możliwość zakażenia się wirusem. Jako producent m.in. systemów przyzywowych i komunikacji dla placówek medycznych możemy podać przykład realizacji szpitala zakaźnego w Moskwie, którego konstrukcja zajęła tylko jeden miesiąc. W obiekcie zainstalowano system VISOCALL IP – pierwszy certyfikowany zgodnie z normą DIN VDE 0834 system przyzywowy i komunikacji. Dzięki swojej budowie i funkcjonalności spełnia on wymagania do stosowania w szczególnych – takich jak pandemia – warunkach. Innowacyjny system oparty na standardzie IP jest elastyczny w konfiguracji, jego zastosowanie umożliwia pełne wykorzystanie istniejącej infrastruktury technicznej poprzez łatwą integrację z innymi systemami.

Całe przedsięwzięcie wymagało niestandardowego podejścia zarówno do budowy obiektu (reżim sanitarny), jak i do projektowania jego struktury oraz zastosowanych technologii (izolacja zakaźnych). Wszystkie pomieszczenia pacjentów zostały całkowicie odizolowane (zablokowano wejścia i wyjścia), a jedynym sposobem komunikacji pacjentów z personelem medycznym były terminale systemu przyzywowego (dzięki prostej dezynfekcji i możliwości komunikacji głosowej). System VISOCALL IP ma wiele istotnych cech, szczególnie ważnych podczas planowania i projektowania rozwiązań szpitalnych w czasach takiego zagrożenia, jakim jest COVID-19. Po pierwsze wszystkie urządzenia są wykonane z materiałów wysokiej jakości (tworzyw sztucznych i powłok) zapewniających stałą ochronę przed zanieczyszczeniem bakteryjnym, działającym przeciwdrobnoustrojowo, bez zbędnych szwów i wystających przycisków lub przetłoczeń, które sprzyjałyby gromadzeniu się niehigienicznych złożeń. Możliwość dezynfekcji jest potwierdzona przez Europejski Interdyscyplinarny Komitet Badań Higieny i Zgodności Wyrobów Medycznych (EICHY). Dzięki temu urządzenia można bezpiecznie czyścić i dezynfekować.

Ważną cechą VISOCALL IP jest możliwość ograniczenia do minimum kontaktów pomiędzy personelem a pacjentami dzięki wykorzystaniu systemu z funkcją rozmowy i rozgłaszania komunikatów. Rozwój technologiczny pozwolił rozszerzyć funkcjonalność systemów przyzywowych z tra-



dycyjnej komunikacji werbalnej do wygłaszania komunikatów, a nawet umożliwił dostęp do telewizji, radia, Internetu bądź telefonu w przyłózkowym terminalu pacjenta.

Technologia sieciowa IP gwarantuje pełną funkcjonalność nawet podczas uszkodzenia serwera oraz prowadzenie rozmów z poszczególnymi pacjentami w tym samym czasie – w sposób dyskretny przy użyciu słuchawek lub głośnomówiących, gdy słuchawki zamontowane są w uchwycie na ścianie. Natomiast odbieranie przywołań odbywa się za pomocą urządzeń systemowych w punktach pielęgniarskich, pomieszczeniach personelu lub innych salach, a także na telefonach przenośnych DECT/VoIP. Wszystkie te urządzenia muszą zapewniać odbieranie przywołań, prowadzenie rozmów, akceptowanie lub zdalne kasowanie przywołań po zakończeniu rozmowy.

Ponadto system VISOCALL IP pozwala na wykorzystanie słuchawek pacjenta oraz terminali pielęgniarskich jako telefonów SIP poprzez integrację z centralą telefoniczną. Rozwiązanie to daje pacjentowi możliwość bezpośredniego kontaktu ze swoimi bliskimi. Dzięki takiej funkcjonalności izolacja pacjentów, która często ma negatywny wpływ na ich samopoczucie, staje się łatwiejsza do zniesienia.

Należy pamiętać, że komunikacja głosowa pomiędzy personelem świadczącym opiekę a pacjentami za pośrednictwem terminali, które znajdują się przy ich łóżkach, musi spełniać zało-

żenia Rozporządzenia o Ochronie Danych Osobowych (RODO) i ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (patrz artykuł w nr 1/2020 „a&s Polska”). Wielu producentów systemów przyzywowych bazuje na rozwiązaniach interkomowych przy łóżku chorego zamiast słuchawek. Zgodnie ze wspomnianym rozporządzeniem uniemożliwia to przekazywanie informacji wrażliwych pacjentowi, a jak wiadomo, takich komunikatów związanych m.in. ze stanem zdrowia pacjenta w szpitalach jest wiele.

Technologia IP otwiera również możliwość integracji z wieloma perspektywicznymi rozwiązaniami, takimi jak urządzenia przywoławcze przeznaczone dla osób najbardziej potrzebujących lub niepełnosprawnych. Terminale pacjentów (w formie słuchawki) umożliwiają podłączenie w dowolnej chwili przenośnych pętli indukcyjnych służących do komunikacji z osobami słabosłyszącymi, spełniając tym samym wymagania projektu rządowego „Program Dostępność Plus”, przedstawionego na stronie Kancelarii Prezesa Rady Ministrów; wymagania są opisane w ustawie z 19 lipca 2019 r. o zapewnieniu dostępności osobom ze szczególnymi potrzebami.

Funkcjonalność systemu przyzywowego można rozszerzyć poprzez integrację z innymi systemami, np. urządzeniami medycznymi, centralami sygnalizacji pożarowej, serwerami alarmów, systemami rozliczeniowymi, systemami lokalizacji, centralami telefonicznymi, telefonami DECT/VoIP, pagerami itp.

Proponowane przez Schrack Seconet rozwiązania pozwalają na dopasowanie się do potrzeb pacjentów i innych użytkowników, szczególnie teraz, gdy mamy do czynienia z licznymi ograniczeniami w kontaktach personelu medycznego z pacjentami, osobami starszymi w domach pomocy społecznej i innych placówkach tego typu. Przytoczony przykład zrealizowanego obiektu – szpitala w Moskwie – potwierdza, że zastosowanie systemu kompletnego, spełniającego wszystkie wymogi prawne i użytkowe oraz niezawodnego, w znacznym stopniu zwiększa szansę na powodzenie w sprawniej realizacji projektu oraz bezpieczeństwo personelu i pacjentów. ▣

* <https://aspolska.pl/komunikacja-za-pomoca-systemow-przyzywowych-a-ochrona-prywatnosci-i-godnosci-pacjenta/>



**Schrack
Seconet
Polska**

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



Zastępcze miejsca szpitalne w budynkach użyteczności publicznej

LONDYN (ANGLIA), CENTRUM WYSTAWIENNICZE EXCEL.

WIOSNA 2019 R. - MIĘDZYNARODOWE TARGI ŚLUBNE.

WIOSNA 2020 R. - SZPITAL POŁOWY NA 4 TYS. ŁÓŻEK¹.

MADRYT (HISZPANIA), HOTEL NH PARLA.

WIOSNA 2019 R. - POKOJE ZAJĘTE PRZEZ TURYSTÓW.

WIOSNA 2020 R. - 88 POKOI GOTOWYCH NA PRZYJĘCIE PACJENTÓW CHORYCH NA COVID-19.

TO NOWA RZECZYWISTOŚĆ, W KTÓREJ WSZYSCY MUSIMY SIĘ ODNALEŻĆ. STADIONY PRZESTAŁY WYPEŁNIAĆ SIĘ KIBICAMI, A ZACZYNAJĄ PRZYJMOWAĆ PACJENTÓW.



T E K S T
Łukasz Stępień

31 grudnia 2019 r. będzie datą pamiętną. Tego dnia komitet ochrony zdrowia z Wuhan przekazał informację Światowej Organizacji Zdrowia (WHO) o zachorowaniu 27 osób na zapalenie płuc o nieznanym etiologii². Powodem choroby okazał się koronawirus SARS-CoV-2, wywołujący jednostkę chorobową COVID-19³. Liczba chorych przerosła pojemność systemu ochrony zdrowia w wielu krajach. Nie można udzielić pomocy wszystkim potrzebującym. I tak naprawdę to nie zakażenie SARS-CoV-2, ale niewydolność systemu ochrony zdrowia jest największym zagrożeniem dla społeczności. W szumie medialnym wokół epidemii łatwo się bowiem zapomina, że COVID-19 nie jest jedynym zagrożeniem życia i zdrowia. System ochrony zdrowia musi wciąż leczyć ludzi chorych na nowotwory, ofiary wypadków, udarów mózgu czy zawałów serca. Każde łóżko w szpitalu jednoosobowym, przeznaczonym dla osób chorych na COVID-19, to jedno łóżko mniej dla innych pacjentów. W takich warunkach np. zapalenie wyrostka robaczkowego, które przed epidemią było operowane w ciągu kilku godzin, dziś może stanowić śmiertelne zagrożenie życia i zdrowia.

Wiele państw na początku epidemii podjęło decyzję o uruchomieniu planów kryzysowych i przekształceniu wybranych obiektów użyteczności publicznej w zastępcze miejsca szpitalne (ZMSz). Luksusowe hotele, hale targowe i domy studenckie pełnią funkcję tymczasowych szpitali. Izolowanie jednego typu pacjentów w jednym obiekcie nie tylko odciąża system ochrony zdrowia, ale też zwiększa efektywność zarządzania posiadanymi zasobami, ponieważ ich dystrybucja sku-

pia się na kilku głównych ośrodkach. Na co zwracać uwagę podczas doboru obiektu mającego pełnić funkcję szpitala zastępczego? Podstawowym założeniem przy niezbędnych adaptacjach jest maksymalne wykorzystanie istniejącej infrastruktury i wprowadzenie jak najmniejszych modyfikacji. Takie podejście oszczędza nie tylko liczebność personelu i zasoby materialne, ale także przyspiesza uruchomienie obiektu w jego nowej funkcji.

Niezależnie od tego, czy jest to wyspecjalizowany szpital zakaźny, czy świeżo zaadaptowana hala targowa, WHO rekomenduje zastosowanie schematu organizacyjnego dzielącego obiekt na dwa sposoby. Pierwszy to podział na trzy obszary funkcyjne: poczekalnia, oddział i strefy dla personelu. Poczekalnia stanowi funkcję „wejścia” do obiektu. Jest tam prowadzona rejestracja i ocena (triage) stanu zdrowia pacjentów oraz, w razie potrzeby, pobiera się próbki do dalszych badań. Zależnie od przyjętej polityki pacjenci w lepszym stanie mogą trafiać na oddziały izolacyjne w oczekiwaniu na wyniki albo być kierowani do domów, gdzie będą poddani kwarantannie aż do uzyskania wyniku testów. Osoby w cięższym stanie trafiają na oddziały, gdzie jest udzielana im pomoc w oczekiwaniu na diagnostykę. Ze względów epidemiologicznych⁴ system organiza-

cji pracy w poczekalni powinien zapewnić odstęp 2 m pomiędzy osobami oczekującymi na kontakt z lekarzem. Dystans można zmniejszyć, jeżeli zastosuje się ekrany lub kotary oddzielające.

Drugi obszar stanowią oddziały, na których przebywają pacjenci. W szpitalach są to często oddziały dla pacjentów z różnymi schorzeniami i w różnym stanie. W przypadku obiektów pełniących funkcję szpitalnych miejsc zastępczych podejmuje się starania, by w sposób maksymalny standaryzować poziom opieki. W praktyce najczęściej funkcjonuje podział na trzy poziomy specjalizacji: pacjenci samodzielni potrzebujący doraźnej kontroli, pacjenci samodzielni wymagający wsparcia terapeutycznego oraz pacjenci w stanie ciężkim wymagający wsparcia ze strony respiratora.

Trzeci wydzielony obszar stanowi strefę dla personelu, w której znajdują się szatnie, toalety, magazyny i apteka. Również na oddziałach mogą znajdować się wyłączone strefy dla personelu. Uproszczony schemat organizacyjny pokazano na rys 1.

4) Objawy COVID-19 są podobne np. do objawów grypy i przebiegają, dlatego jest duże prawdopodobieństwo, że do poczekalni trafią osoby, które nie mają SARS-CoV-2.

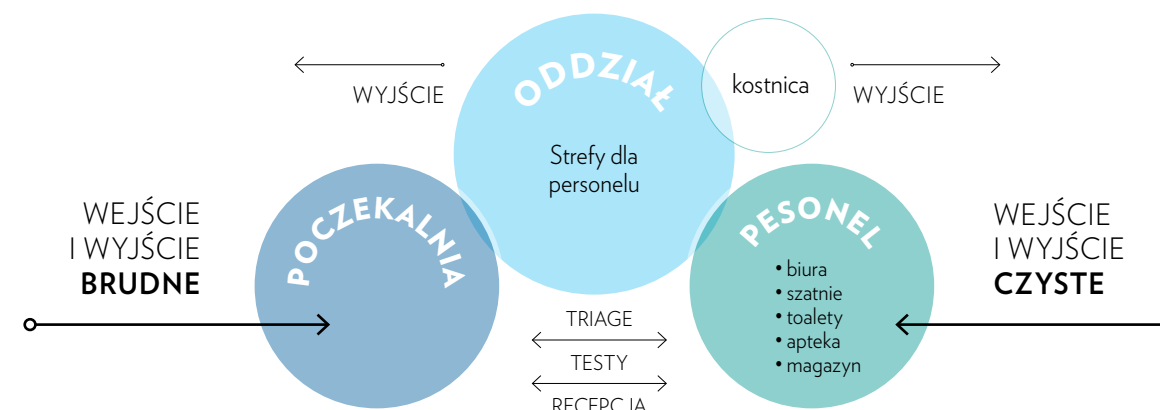
Drugi sposób to podział obiektu na dwie „święte” strefy: brudną i czystą. Strefa brudna obejmuje poczekalnię i oddziały szpitalne, do których dostęp mają personel medyczny i pacjenci. Do strefy czystej dostęp ma tylko personel szpitalny. Celem całej logistyki przepływu pacjentów i materiałów jest zachowanie niezależności obu stref. Obiekt powinien mieć zapewnione co najmniej trzy niezależne i oddalone od siebie wejścia: dla pacjentów, personelu medycznego oraz miejsce rozładunku dostaw z lekami i wyposażeniem. Ponadto zdrowi pacjenci powinni móc opuszczać oddział bez przechodzenia przez recepcję, by zminimalizować ryzyko zakażenia. Część obszarów, m.in. recepcja, pomieszczenie do oceny stanu pacjenta czy pobierania próbek leży na styku strefy czystej i strefy brudnej, dlatego WHO rekomenduje zorganizowanie do nich osobnych wejść dla personelu i osobnych dla pacjentów. Podział na strefy czyste i brudne nie tylko ogranicza ryzyko zakażeń personelu szpitalnego, ale także pozwala na bardziej racjonalne zużywanie środków ochrony osobistej.

Ocena przydatności danego obiektu

powinna być prowadzona na podstawie aktualnej dokumentacji budynku, która uwzględnia wszystkie plany obiektu wraz z instalacjami sanitarnymi, wentylacyjnymi i elektrycznymi. Tylko taka kompletna dokumentacja może stanowić podstawę do dalszych działań. Warto również sprawdzić, czy są realizowane wszystkie przeglądy spoczywające na właścicielu obiektu. Budynki piętrowe powinny być wyposażone w windę, której rozmiar umożliwia transport pacjenta na noszach z zespołem medycznym. Korytarze powinny mieć szerokość pozwalającą na swobodne manewrowanie noszami. Jeżeli w obiekcie uwzględniono miejsca dla pacjentów leżących, szerokość korytarza powinna umożliwiać mijanie się dwóch łóżek szpitalnych, a winda, oprócz odpowiedniej szerokości, musi mieć udźwieg pozwalający na transport łóżka szpitalnego z wyposażeniem i personelem medycznym. Wielkość pomieszczeń przeznaczonych dla pacjentów musi uwzględniać, oprócz łóżka, również miejsce do swobodnej pracy personelu medycznego ubranego w komplet środków ochrony indywidualnej. WHO rekomenduje przyjęcie standardu 10 m² na jednego pacjenta leżącego oraz niezależny węzeł sanitarny przypisany do danego pomieszczenia.

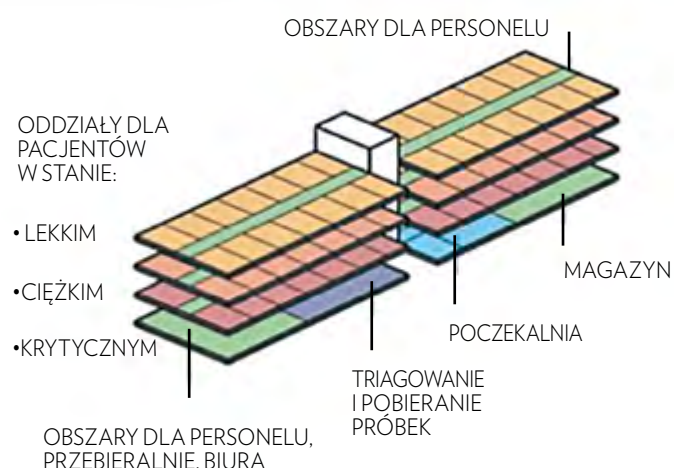
Kolejnym elementem jest ocena, jak dużego zaangażowania wymagałoby dostosowanie pomieszczeń do wymogów sanitarno-epidemiologicznych. W środowisku lekarzy zakaźnych krąży powiedzenie „im większy komfort pacjenta, tym więcej powierzchni do dezynfekcji”, dlatego wyposaże-

RYŚ. 1. **UPROSZCZONY SCHEMAT ORGANIZACYJNY SZPITALA ZAKAŻNEGO**



1) Dla właściwego odniesienia skali – największy w Polsce szpital, Krakowski Szpital Uniwersytecki, dysponował w 2016 r. 1560 łóżkami dla pacjentów.
2) Etiologia – przyczyna choroby.
3) Stosowane nazwy są skrótami z j. angielskiego: Sars CoV-2 – Severe acute respiratory syndrome CoronaVirus 2, COVID-19 – Coronavirus disease 2.

RYS. 2. **DOSTOSOWANIE HOTELU DO FUNKCJI ZASTĘPCZYCH MIEJSC SZPITALNYCH. MATERIAŁY ZE SZKOLENIA WHO SARI FACILITIES.**



nie sali pacjenta powinno być zredukowane do minimum i łatwe do dezynfekcji. Należy usunąć elementy o porowatej powierzchni czy wykonane z materiałów mogących chłonić wilgoć. Dotyczy to np. dywanów, ciężkich kotar i zasłon. Korpus inżynierów armii USA w swojej publikacji *Hotel to Health Care Concept*⁵ zaleca, aby wyposażenie pokoju ograniczało się do szafki dla pacjentów, mobilnego stolika do wykorzystania przez personel medyczny, stojaka do kroplówek, kosza na zabrudzone przedmioty, pojemnika na skażone odpady oraz miejsca do dezynfekcji rąk. Ze względu na komfort psychiczny pacjenci powinni posiadać (w miarę możliwości) prywatny telefon i komputer. Przez cały okres izolacji będzie to ich jedyne „okno na świat”. Dlatego kolejnym elementem, wartym rozważenia, jest dostęp do szerokopasmowego Internetu bezprzewodowego. Dostęp do sieci będzie również niezbędny dla personelu medycznego w realizacji zadań administracyjnych. Wirus SARS-CoV-2 roznosi się drogą kropelkową, czyli z kropelkami śliny i (prawdopodobnie) aerozolu wydobywających się z ust. Ważnym elementem zapobiegającym rozprzestrzenianiu się tego typu zakażeń w pomieszczeniach zamkniętych są systemy wentylacyjne, które umożliwiają regulację przepływu powietrza w budynku. Zwiększenie liczby wymiany powietrza wewnątrz pomieszczenia „rozrzedza stężenie” czynnika zakaźnego. Dzięki utrzymywaniu w pomieszczeniu podciśnienia (więcej powietrza jest odciągane niż nawiewane) ogranicza się

ilość powietrza wydostającego się poza pomieszczenie⁶. Rekomenduje się też założenie dodatkowych filtrów na wentylatory (zależnie od budowy instalacji), jednak ograniczają one przepływ powietrza i wydajność central wentylacyjnych. Wydajność central może być również parametrem limitującym, może się np. okazać, że utrzymanie odpowiednich parametrów jest możliwe tylko w 1/3 spośród wszystkich dostępnych pomieszczeń, co automatycznie ogranicza użyteczną pojemność miejsca jako ZMSz.

Zespół przeprowadzający ocenę budynku powinien określić potrzebę montażu dodatkowych gniazdek elektrycznych w obszarze zarówno przeznaczonym dla personelu (kwestie administracyjne), jak i pacjentów (sprzęt medyczny). Wydawałoby się, że to banalny problem do momentu, kiedy zabraknie wtyczki do podłączenia respiratora. Analiza powinna również obejmować całą instalację elektryczną, czy ma wystarczającą moc przyłączeniową i jest dostosowana do długotrwałego obciążenia przez aparaturę medyczną (pompy insulinowe, kardiomonitorzy czy wspomniane respiratory) oraz dodatkowe oświetlenie. Obiekty przeznaczone dla pacjentów w najcięższym stanie muszą być wyposażone w niezależne agregaty prądu, aby nawet krótkie przerwy w zasilaniu nie stanowiły zagrożenia dla pacjentów.

Na takich oddziałach należy również uwzględnić dostęp do tlenu medycznego. Rozwiązaniem optymalnym byłoby podłączenie się do instalacji już istniejącej lub tymczasowy montaż zbiornika z tlenem wraz z systemem doprowadzającym do poszczególnych łóżek. Mniej efektywną alternatywą jest bazowanie na przewoźnych butlach z tlenem. Mimo że tlen nie jest gazem wybuchowym, to jest silnie utleniający (wspomaga proces spalania). Z tego względu należy bardzo rozważyć ocenę możliwości jego bezpiecznego składowania i wykorzystywania. Należy również przewidzieć miejsce do składowania odpadów zakaźnych i wyrobów farmaceutycznych, np. leków.

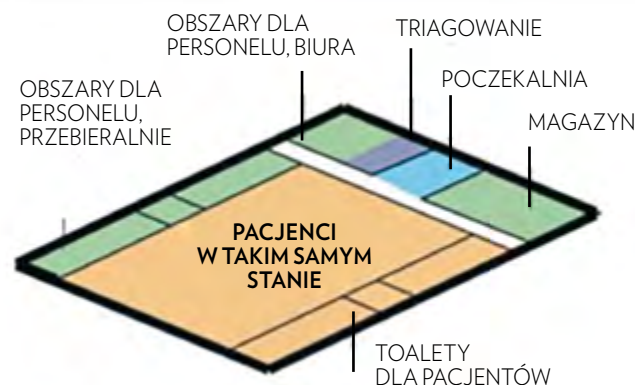
Dojazd do obiektu pełniącego funkcję ZMSz musi zapewniać swobodę w manewrowaniu karetom pogotowia i pojazdom z dostawami. W przypadku obiektów otwartych, do których pacjenci mogą samodzielnie się zgłaszać, należy też uwzględnić odpowiednią liczbę miejsc parkingowych, aby prywatne samochody nie blokowały dojazdu jednostkom ratowniczym.

Dostęp do budynku powinien być ograniczony, a wejście oraz wyjście ściśle kontrolowane, aby zminimalizować ryzyko wyjścia poza teren pacjentów odbywających kwarantannę lub wtargnięcia osób trzecich (np. rodzin pacjentów albo dziennikarzy). Dostosowanie obiektu do funkcji zastępczych miejsc szpitalnych nie może mieć negatywnego wpływu na bezpieczeństwo jego użytkowników. Dlatego należy zawczasu również przemyśleć tak „oczywiste” zagadnienia, jak ewakuacja z budynku w przypadku pożaru. Ze względu na obecność osób będących nosicielami chorób zakaźnych ewakuacja wymaga szczególnych procedur. W takiej sytuacji dodatkowe „punkty” powinny być przyznane lokalizacjom o dużej liczbie niewielkich stref pożarowych.

Jako ZMSz najczęściej brane są pod uwagę wielopiętrowe obiekty noclegowe (hotele, domy studenckie) oraz obiekty przestrzenne (stadiony, hale wystawiennicze), gdyż dysponują odpowiednim zapleczem. Budynki te mają zazwyczaj podobny układ pomieszczeń na wszystkich piętrach oraz część recepcyjno-administracyjną i konferencyjną na parterze. Dodatkową przewagą hoteli jest dostęp do zaplecza gastronomicznego, które można wykorzystać na potrzeby zarówno pacjentów, jak i personelu medycznego. Na rys. 2 podano przykład reorganizacji hotelu na potrzeby ZMSz. Na parterze znajdują się recepcja oraz miejsce do oceny stanu pacjentów. Sale konferencyjne służą za magazyny, a stołówka pełni funkcję pokoju socjalnego dla personelu.

Z kolei hale sportowe i pawilony targowe to obiekty wyjątkowo łatwe do dostosowania ze względu na ich otwartą budowę. W przypadku

RYS. 3. **DOSTOSOWANIE HALI WYSTAWIENNICZEJ DO FUNKCJI ZMSZ. MATERIAŁY ZE SZKOLENIA WHO SARI FACILITIES**



hal wystawienniczych dużym ułatwieniem jest założenie architektoniczne, umożliwiające tworzenia dużej liczby stoisk w różnych konfiguracjach, z dostępem do zasilania elektrycznego. Takie stoiska, po drobnych modyfikacjach, można łatwo zaadaptować na pokoje dla pacjentów w ciężkim stanie. Zastosowanie przezroczystych kurtyn umożliwia kontrolę wielu stanowisk przez jedną osobę z personelu medycznego. Grupa BDP, odpowiadająca za transformację londyńskiej hali widowiskowej ExCel, wydała krótki przewodnik, jak dostosowywać hale widowiskowe na potrzeby zastępczych miejsc szpitalnych. Co ciekawe, przewodnik został wydany w formie graficznej przypominającej instrukcję do składania mebli.

Obiekty sportowe i targowe z zasady są projektowane z podziałem na część oficjalną, przeznaczoną dla widzów i gości, oraz część użytkową dla obsługi obiektu. Ułatwia to logistykę przepływu osób na terenie ZMSz zgodnie z zasadami oddzielenia strefy czystej i strefy brudnej oraz organizacji niezależnych wejść dla personelu, pacjentów, punktu rozładunku dostaw i wjazdu jednostek pogotowia. Przykładowy model organizacji zastępczego szpitala w hali targowej przedstawiono na rys. 3 – cała powierzchnia wystawiennicza jest tu przeznaczona dla pacjentów.

Zastępcze miejsca szpitalne nigdy nie będą miały tak dobrej funkcjonalności jak tradycyjne szpitale. Są one uruchamiane tylko w sytuacjach kryzysowych, kiedy nie ma możliwości wyboru pomiędzy rozwiązaniami dobrymi a złymi. Często trzeba wybierać między rozwiązaniem złym a umiarkowanie złym. Dlatego w proces analizy i doboru właściwych miejsc powinien być zaangażowany zespół specjalistów, prowadzony przez osobę o odpowiednich kompetencjach, aby można było wskazać miejsca o optymalnej funkcjonalności. Tego procesu nie można realizować w zaciszu gabinetów, gdyż plany na papierze mogą nie wytrzymać zderzenia z rzeczywistością.

Dziękuję za konsultację Sergiuszowi Parszowskiemu z Instin.pl, autorowi koncepcji zastępczych miejsc szpitalnych dla miasta Kielce. □

B I O

Łukasz Stępień

Ratownik Medyczny. Specjalista z zakresu bezpieczeństwa pożarowego i zarządzania kryzysowego. Członek Krajowego Stowarzyszenia Ochrony Przeciwpowodzi w USA.



Gwarantujemy wysoką dostępność,
najlepsze wsparcie techniczne oraz
atrakcyjne warunki handlowe



Zapraszamy do współpracy!

(32) 346 30 06
handlowy@promitel.pl
Bocheńskiego 99, Katowice

5) Publikacja US Army Corps of Engineers z 22 marca 2020 r.
6) Jest to rozwiązanie stosowane m.in. w restauracyjnych kuchniach, dzięki podciśnieniu powietrze z kuchennymi zapachami nie przedostaje się do sali dla gości.

Smart city w dobie koronawirusa

TECHNOLOGIE SMART CITY MOGĄ W ZNACZNYM STOPNIU PRZYZYNIĆ SIĘ DO ZWIĘKSZENIA BEZPIECZEŃSTWA I WYKSZTAŁCENIA NOWYCH ZACHOWAŃ SPOŁECZNYCH W CZASIE EPIDEMII. TECHNIKI I TECHNOLOGIE SMART CITY BAZUJĄ NA ROZWIĄZANIACH BEZSTYKOWYCH, BEZPRZEWODOWYCH, ZBLIŻENIOWYCH, A TAKŻE KORZYSTAJĄ Z ŁĄCZNOŚCI INTERNETOWEJ W ROZWIĄZANIACH PRZEWODOWYCH I BEZPRZEWODOWYCH.

Nie wymagają bezpośredniego kontaktu fizycznego osób, są więc bezpieczne. Już na poziomie operacyjnym obywatele mogą korzystać za pomocą swoich smartfonów z e-metod komunikacji z urzędami miejskimi, udostępniać swoją lokalizację, a także przekazywać dane i informacje. Telefonia mobilna ułatwia korzystanie z rozkładów jazdy wszystkich środków komunikacji miejskiej, umożliwia kierowanie tłumem, identyfikację liczby pasażerów w środkach komunikacji miejskiej, pozwala na korzystanie ze zdalnego zamawiania potraw czy też robienia zakupów w wirtualnym sklepie. Niedługo zapewne stanie się możliwe dostarczanie przesyłek w granicach miasta za pomocą dronów. Bezstykowe i bezprzewodowe technologie smart city umożliwią bezpieczne monitorowanie parametrów zdrowia ludzi, lokalizację osób, z dokładnym odtworzeniem trasy ich przemieszczania się, a nawet sposobu bytności osób starszych.

Każde miasto działa przy pomocy swoich urzędów i urzędników. Epidemia wymusiła zmiany w systemach pracy instytucji. Tam, gdzie to możliwe, wprowadzono pracę zdalną. Powstały nawet specjalne metody oceny skuteczności pracy zdalnej urzędników. Na szczęście okazało się, że społeczeństwo jest w większości przypadków wyposażone w najważniejsze obecnie urządzenie, to znaczy komputer z odpowiednim oprogramowaniem. Większość spraw można załatwić przez Internet, nie wychodząc z domu. Rynek oprogramowania szybko zareagował, udostępniając różne aplikacje umożliwia-

jące w urzędach zdalną komunikację czy to w postaci tak zwanych e-platform, pokoiów konferencyjnych, terminali wideokonferencyjnych, czy aplikacji komunikacji wizyjnej w urzędach, teleprezentacji oraz wirtualizacji dokumentów. Większość komunikatorów multimedialnych umożliwia, że widzimy się i słyszymy. Ale trzeba pamiętać, że postęp w systemach wideokonferencyjnych niesie również nowe zagrożenia związane z ochroną danych wrażliwych, które pojawiają się w czasie takich wirtualnych spotkań. Cyberbezpieczeństwo jest współcześnie najtrudniejszą do zapewnienia metodą ochrony danych, bardzo często zabezpieczenia pojawiają się po materializacji zagrożenia.

Tak duży jak obecnie rozwój epidemii na całym świecie wpłynie zapewne na szybki rozwój telemedycyny i monitorowania obszarów o dużych skupiskach ludzi w aspekcie możliwości rozsiewania zakażeń, rozwoju choroby, a także na organizację przebywania osób (choćby starszych). Wszystkie znane dziś technologie, stanowiące dotychczas gadżety, będą rozpatrywane w kategoriach standardów. Możliwość zdalnego pomiaru temperatury ciała (za pomocą kamer termowizyjnych) i zdalnej wymiany danych w centralnym systemie ochrony zdrowia, a także sposobność zdalnej oceny innych parametrów życiowych człowieka ułatwi zdiagnozowanie oraz przewidzenie rozwoju choroby czy zakażenia w obserwowanej społeczności, od mieszkańców bloków po mieszkańców dzielnic. Pozwoli to chronić i ostrzegać ludzi zdrowych, chroniąc jednocześnie i izolując osoby zarażone.

Urządzenia mobilne i media społecznościowe umożliwią stały kontakt z osobami zarówno zdrowymi, jak i izolowanymi, zapewnią dostawę żywności i innych niezbędnych środków, umożliwiając także zgłaszanie zapotrzebowania, a w niedalekiej przyszłości poprzez system inteligentnej lodówki.

Rozwinie się zapewne jeszcze bardziej e-handel, a za nim e-płatności. Już dzisiaj coraz częściej słyszy się o możliwości rezygnacji z pieniądza fizycznego na korzyść pieniądza wirtualnego. Metody bezprzewodowych płatności czy e-portfela umożliwiają zakupy biletów, realizację płatności w sklepach czy instytucjach publicznych. Rozwinie się również ważny element życia ludzi w społeczeństwie w postaci ich integracji z mediami spo-



T E K S T
Prof. Jerzy Mikulik

ZOBACZ KAŻDY SZCZEGÓŁ



Wisenet P series

Kamery Wielo-przetwornikowe Wisenet P to rozwiązanie do otwartych przestrzeni.

- Obserwacja całego obszaru bez "martwych" stref
- Rozdzielczość do 20MP zapewniająca szczegółowy obraz
- Zmniejszenie liczby kamer i redukcja kosztów instalacji
- H.265 i WiseStream redukują pasmo i wymaganą przestrzeń dyskową

Stworzyliśmy kamery Wielo-przetwornikowe Wisenet Premium, żeby nigdy nie umknął Ci żaden szczegół.

Zobacz więcej na
www.hanwha-security.eu/wisenet-p



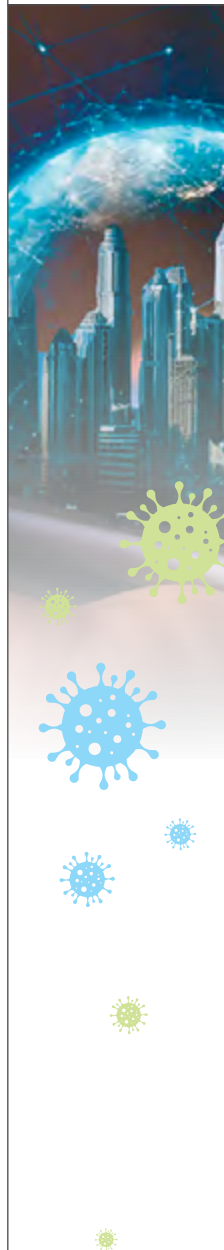
lecnościowymi. Dokona się to za pomocą popularnych w przestrzeni publicznej komunikatorów. Coraz bardziej dostępna rozszerzona rzeczywistość będzie podpowiadała o dostępności i możliwości zakupu różnych produktów, np. biletów do kina (z zachowaniem chociażby zasad bezpieczeństwa w kinie), możliwości wirtualnego przymierzania odzieży w sklepach i zamawiania ich do domu bez potrzeby kontaktu ze sprzedawcą lub doradcą.

Bardzo ważnym elementem w strukturze *smart city* jest edukacja społeczna na wszystkich poziomach, od szkolnictwa podstawowego, poprzez średnie i zawodowe, po szkolnictwo wyższe i naukę przez całe życie. Zasoby ludzkie biorące udział w procesach nauczania stanowią duże lub bardzo duże grupy. Tutaj bardzo łatwo może zarazić się wiele osób od jednej osoby zakażonej, co było wyraźnie widoczne w kopalniach węgla, gdzie pracują duże zespoły w zamkniętych pomieszczeniach. Całe szkolnictwo musiało zmienić system nauczania na nauczanie zdalne. To wielkie nowe doświadczenie. Na świecie byli i są ludzie uczciwi i nieuczciwi, porządni i nieporządni. Praca zdalna w edukacji wymaga zastosowania bezpiecznej i przyjaznej, a zarazem trudnej do oszukania i wydajnej platformy komunikacyjnej. Można stosować e-platformy statyczne i multimedialne z głosem i dźwiękiem.

Problem jest z udostępnianiem tzw. linków dopuszczających do uczestnictwa w videokonferencji. Zabezpieczenia, jakich używa się obecnie, są za słabe. Link do spotkania można przekazać nieuprawnionej osobie, która może spowodować ogromne zamieszanie w czasie wideospotkania. Pomocna w tym przypadku okaże się kontrola biometryczna, ale to się wiąże z koniecznością używania komputerów czy laptopów wyposażonych w czytniki biometryczne. Takie urządzenia są już dostępne, ale korzystanie z nich nie jest popularne, choć zapewne i to się zmieni.

Należy też wspomnieć o jednym z najważniejszych elementów składowych koncepcji *smart city*, czyli komunikacji. Pojawiają się nowe możliwości zarządzania, kontroli oraz sterowania ruchem drogowym, np. kontrola wjazdu samochodów do miasta, inteligentna nawigacja i sterowanie pasami ruchu, oświetlenie dróg i ścieżek rowerowych. Bardziej powszechne będzie wykorzystanie techniki Light ID do komunikacji z użytkownikami samochodów, rowerów miejskich czy przechodniów. Technika Light ID pozwala na udostępnianie wszelkiego rodzaju informacji za pomocą niewidzialnego promieniowania emitowanego

Trudno dzisiaj ocenić kierunki zmian i konkretne rozwiązania, jakie wyewoluują z dostępnych technologii, ale na pewno będą niezbędne w tworzeniu nowej rzeczywistości po epidemii koronawirusa



przez diody IR. Może służyć do przekazywania treści reklamowych bądź informacyjnych. Aby ją odczytać, wystarczy smartfon z aparatem fotograficznym i odpowiednią aplikacją. Urządzenia mobilne umożliwią przesłanie do służb miejskich informacji o konieczności np. odkażania danych miejsc lub usuwania odpadów ze względu na to, iż przez kilka godzin gromadzili się tam ludzie (mapa koncentracji skupisk ludzkich).

Zapewne wprowadzenie zautomatyzowanego i autonomicznego transportu pozwoli na nowo zorganizować poruszanie się po mieście, wyłączy np. możliwość bezpośredniego kontaktu kierowcy pojazdu z pasażerami, bo po prostu tego kierowcy nie będzie. Sterowanie i zarządzanie pojazdem przejmie sztuczna inteligencja, ale najpierw sztuczna inteligencja musi uzyskać osobowość prawną. Niestety obecna epidemia spowodowała powrót kierowców w miastach do swoich aut. W mieście w samochodzie jedzie przeważnie jedna osoba, a w pojeździe komunikacji miejskiej kilkadziesiąt. Jak widać, prawdopodobieństwo zakażenia się w komunikacji miejskiej jest bardzo duże. Rozwiązaniem problemu zanieczyszczania środowiska będzie możliwość kupna samochodu elektrycznego w rozsądnej cenie.

Trudno dzisiaj ocenić wszystkie kierunki zmian i konkretne rozwiązania, jakie wyewoluują z obecnie dostępnych technologii, ale na pewno będą one niezbędne w tworzeniu nowej rzeczywistości po epidemii COVID-19. Pokazaliśmy, jako społeczeństwo, że praca zdalna pozwoliła pogodzić życie zawodowe z prywatnym. Może też się okazać, iż nie będą potrzebne tak duże przestrzenie biurowe, gdyż już widać, że część prac administracyjnych i biurowych można wykonywać zdalnie, a spotykać się podczas videokonferencji, bez konieczności odbywania podróży. Człowiek jest jednak istotą stadną i źle znosi życie w izolacji, co potwierdzają wykonywane badania socjologiczne. W czasie trwania epidemii, wykonując w rodzinnej izolacji pracę zdalną i przeważnie też uczestnicząc w domowej szkole, ma się do wyboru dwa działania: albo trochę poluzować i odpuszczyć, albo... porażka. I jak tu żyć? ▢

B | O

prof. dr hab. inż. Jerzy Mikulik

Absolwent Wydziału Elektrotechniki, Automatyki i Elektroniki AGH w Krakowie. Obecnie kierownik Katedry Inżynierii Zarządzania, Wydział Zarządzania AGH oraz kierownik Laboratorium Automatyzacji Procesów na tym Wydziale. Przewodniczący KT Facility Management przy PKN oraz kierownik studiów podyplomowych „Facility Management – zarządzanie inteligentnym budynkiem” i „Cyberbezpieczeństwo i zarządzanie bezpieczeństwem informacji” na Wydziale Zarządzania AGH. Od wielu lat zajmuje się teorią i praktyką systemów bezpieczeństwa w budynkach inteligentnych. Autor wielu artykułów i książek dotyczących zarządzania bezpieczeństwem i komfortem w budynkach inteligentnych.

Koncepcja bezpiecznego miasta łączy wiele elementów: innowacyjne wykorzystanie technologii informacyjnej, wydajny parking, zrównoważone zużycie energii i czyste środowisko.



Bezpieczne miasto

↓ według
C&C Partners

Miasta stoją obecnie przed nowymi wyzwaniami. Jedni obywatele skarżą się na jakość powietrza, inni narzekają na problemy związane z ruchem drogowym, parkowaniem, bezpieczeństwem, zmianami klimatu, niedostatecznym dostarczaniem informacji lub wynikające ze stale rosnącej urbanizacji.

Kamery w mieście

Wyniki badań prowadzonych w ostatnich latach potwierdzają, że wraz ze wzrostem wizyjnych systemów dozoru liczba przestępstw diametralnie maleje. Dzięki inteligentnej analizie obrazu z kamer reakcja służb porządkowych może być natychmiastowa, a czas pojawienia się na miejscu zdarzenia wyniesie kilka minut. Świetna jakość nagrań w każdych warunkach, coraz lepsze algorytmy analizy twarzy i zachowania osób („szwendanie się”, pozostawienie bagażu w newralgicznych punktach) pomagają ustalić tożsamość danej osoby.

Zielona Góra bezpiecznym miastem

Świetnym przykładem zrealizowanego przez C&C Partners projektu bezpieczne miasto jest Zielona Góra – mówi Szymon Staszak, kierownik projektu w C&C Partners. Zainstalowany tam inteligentny system monitoringu miejskiego obejmuje 91 punktów kamerowych, rejestrujących 305 strumieni wizyjnych wysokiej roz-

dzielczości. Realizację tego celu umożliwia zastosowanie kamer czteroobiektywowych, które zainstalowano głównie w centrum miasta oraz na newralgicznych skrzyżowaniach ulic. Dodatkowo zastosowano kamery obrotowe wyposażone w oświetlacz podczerwieni o zasięgu 500 m, kamery stałopozycyjne o rozdzielczości 4K oraz obrotową kamerę mobilną, którą można zamontować na pojeździe.

System monitoringu w Zielonej Górze powstał z wykorzystaniem inteligentnej platformy do zarządzania strumieniami wizji, z rozbudowaną analityką obrazu VDG SENSE. Obraz z zainstalowanych kamer jest przesyłany do Centrum Zarządzania, gdzie przez 24 godz. na dobę, 7 dni w tygodniu jest obserwowany przez operatorów, a także transmitowany do komendy policji i siedziby ABW w Zielonej Górze. W identyfikacji zdarzeń online i *post factum* wspomaga operatorów zainstalowana w kamerach inteligentna analiza obrazów, która realizuje następujące funkcje: rozpoznawanie tablic rejestracyjnych, koloru samochodu, twarzy, wieku i płci, identyfikację pozostawionego bagażu, gromadzenie się tłumu.

Bezpieczne drogi

Kamery HIGH-END przeznaczone do identyfikacji tablic rejestracyjnych

oferują wiele unikatowych możliwości, m.in. rozpoznanie tablic rejestracyjnych pojazdów na wielu pasach ruchu jednocześnie, detekcję prędkości pojazdu, rozpoznanie koloru, marki i modelu pojazdu, obliczanie średniego czasu przejazdu. Taka analiza jest możliwa dla pojazdów osiągających prędkość nawet do 250 km/h z dokładnością >95%.

Komunikacja i pierwsza pomoc

Inteligentne słupki rozmieszczone w mieście i zintegrowane z systemem monitoringu wizyjnego, dzięki przyciskowi alarmowemu umożliwiają całodobową komunikację głosową z operatorem systemu i wezwanie pomocy. Pozwalają również na przekazywanie przez system rozgłoszeniowy komunikatów skierowanych do mieszkańców i turystów. Słupki są dostosowane do korzystania przez osoby niepełnosprawne poruszające się na wózku inwalidzkim czy niedosłyszące. Dzięki wbudowanemu urządzeniu AED słupki jest jednocześnie punktem ratunkowym. Każde użycie AED generuje automatyczny alarm u operatora i obraz z miejsca zdarzenia.

Sprawne korzystanie z parkingów

Ze względu na to, że ponad 75% kierowców korzysta już z aplikacji mobilnych, istnieje możliwość wyszukiwania wolnych miejsc parkingowych jeszcze przed przybyciem na miejsce oraz uiszczania opłat za parkowanie za pomocą specjalnej aplikacji inteligentnego parkowania. Aplikacja e-kontrola pozwala zdalnie, za pomocą kamery mobilnej zamontowanej na samochodzie, sprawdzić, czy kierowca uiścił opłatę za postój. ▢

C&C Partners

ul. 17 Stycznia 119, 121,
64-100 Leszno
<https://www.ccpartners.pl>



Smart City

– więcej korzyści dzięki
integracji zasobów

Rozwiązania Smart City wykorzystujące potencjał sztucznej inteligencji i IoT będą się rozwijać. Prawdopodobnie nakłady na innowacyjne technologie w tej dziedzinie mogą nie osiągnąć w 2022 roku zacowanych jeszcze niedawno 158 mld USD¹, ale z pewnością będą rosły, podobnie jak rynek IoT².

Dzięki szybkiemu rozwojowi przetwarzania danych w urządzeniach brzegowych sieci i wykorzystaniu mobilnego Internetu pojawia się wyższa gotowość technologiczna użytkowników. Wraz z nią otwierają się nowe możliwości integracji funkcjonujących już rozwiązań i w efekcie lepsze wykorzystanie dostępnych technologii.

Pomocne dla włodarzy miast i biznesu będą otwarte interfejsy programistyczne łączące urządzenia oraz kreujące kolejne rozwiązania optymalizujące usługi miejskie.

1) <https://channellife.com.au/story/idc-forecasts-smart-city-spending-reach-158-billion-2022>
2) Smart City w UE; szacowana aktywna liczba połączeń IoT w 2019 r. – 6,6 mln euro.
<https://res.cloudinary.com/yumyoshoin/image/upload/v1/pdf/iot-business-2020.pdf>



T E K S T
Konrad Badowski

ekspert smart city Axis Communications

Ze względu na szybko postępującą cyfryzację sfery biznesowej i publicznej, nawet na poziomie relacji, warto spojrzeć świeżym okiem na kwestie Smart City. Punktem odniesienia rozważań będą rozwiązania dozoru wizyjnego ze względu na ich dostępność i powszechność stosowania.

Spodziewamy się, że inwestycje w obszarze monitoringu wizyjnego będą miały w najbliższym czasie bardzo indywidualny charakter dyktowany konkretnymi potrzebami społeczności lokalnej – gminy, powiatu i miasta. Największym wyzwaniem będzie maksymalne wykorzystanie dostępnych zasobów i pełni ich możliwości. Użytkownicy i administracja będą poszukiwać nowych możliwości praktycznych zastosowań istniejącej infrastruktury. Odpowiedzią na dodatkowe funkcje i potrzeby czy automatyzację dostępnych narzędzi będzie ich integracja. Procesy utrzymania i lepszego wykorzystania technik i technologii inteligentnego miasta będą wymagały eksperckich konsultacji z rynkiem – integratorami technologicznymi. Organizacje już teraz zwracają się w stronę otwartych technologii.

Przykłady integracji

Smart City będzie potrzebowało ekonomicznego planowania zasobów. W transporcie miejskim efektywność wykorzystania taboru może zwiększyć np. analiza zapelnienia autobusów czy tramwajów w czasie rzeczywistym. Spółki transportu miejskiego będą wspierać się wysokiej jakości danymi w zarządzaniu taborem i ruchem. Można się także spodziewać, że ze względów bezpieczeństwa wzrośnie rola przepływu informacji pomiędzy służbami miasta, spółkami transportowymi i policją – na temat wypadków, dużych zgromadzeń, wyłączenia odcinków ulic z ruchu czy remontów.

Językiem u wagi staje się także gospodarowanie powierzchnią parkingową na poziomie dzielnic i aglomeracji – inteligentne miasta mogą z niej czerpać regularne przychody obciążone niewielkim kosztem pozyskania. Dostępne już systemy monitoringu wizyjnego mogą rozpoznawać tablice rejestracyjne, a nawet rozróżniać pojazdy, przyznając im prawo wjazdu na parking lub naliczając opłaty – odpowiednio mieszkańcom, pojazdom służbowym/komercyjnym, uprzywilejowanym czy służbom bezpieczeństwa. Integracja istniejących rozwiązań z nowymi aplikacjami poprzez otwarte platformy programistyczne umożliwi automatyzację procesów – od poboru opłat, po aktualną informację o ich statusie do systemów finansowych.

Uważnie obserwujemy kolejny obszar usług, który będzie wymagał inteligentnego gospodarowania odpadami miejskimi. Nie wykluczamy, że coraz surowsze wymogi segregowania śmieci oraz higieny i bezpieczeństwa składowania skierują tę dziedzinę w stronę cyfryzacji właśnie poprzez integrację. Podrzucanie śmieci, niewłaściwe segregowanie staje się zmartwieniem wspólnot, spółek komunalnych i obywateli. Zyskują na znaczeniu prywatne systemy monitoringu wizyjnego w tej dziedzinie. I znowu połączenie sił poprzez integrację rozwiązań będzie wspierało społeczność lokalną.

Nowoczesne kamery – urządzenia brzegowe sieci – podobnie jak smartfony można wyposażać w różnego typu aplikacje i sensory, m.in. dając im możliwość nadawania komunikatów audio, analizowania sytuacji, uruchamiania zdarzeń, np. alarmów. Dzięki takim funkcjonalnościom miejski system monitoringu wizyjnego (a także kamery zlokalizowane na terenach prywatnych i w zakładach przemysłowych) staje się dodatkowym, cybernetycznym zesta-

wem „zmysłów” miasta. Dzięki niemu można potwierdzać informacje (dane) otrzymywane od innych systemów lub odpowiednio łączyć obrazy z komunikatami dźwiękowymi.

Integracja jest naturalnym procesem stopniowego, coraz szerszego wykorzystywania możliwości istniejącej infrastruktury. Kluczowe pozostają zgodność produktów i tworzenie niezawodnych rozwiązań sieciowych. Powszechny staje się dostęp do otwartych interfejsów programistycznych, narzędzi i dokumentacji technicznej, zestawów *Software Development Kit* oraz indywidualnego wsparcia. Znacznie ułatwia to dziś twórcom oprogramowania integrację szerokiej gamy istniejących już rozwiązań monitoringu wizyjnego. Inteligentne aplikacje wizyjne do urządzeń brzegowych to przyszłość inteligentnego miasta. □



**Axis Communications
Poland**

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





W poszukiwaniu miasta inteligentnie bezpiecznego

**BEZPIECZEŃSTWO JEST CORAZ
CZĘŚCIEJ TEMATEM DYSKUSJI
W KONTEKŚCIE BUDOWANIA
STRATEGII INTELIGENTNYCH
MIAST. CZY JEDNAK WSZYSCY
JEDNAKOWO ROZUMIEJĄ
POJĘCIE BEZPIECZEŃSTWA?
CZY EKSPERCI OD
BEZPIECZEŃSTWA I MIESZKAŃCY
WIDZĄ PROBLEM PODOBNIIE?
CO ZROBIĆ, ABY MIASTA STAŁY SIĘ
INTELIGENTNIE BEZPIECZNE?**

N

Nie ma jednej definicji miasta inteligentnego. Na potrzeby artykułu proponuję przyjąć, że idea *smart city* to koncepcja zarządzania współczesnym miastem w duchu zrównoważonego rozwoju, angażującego możliwie największą liczbę jego użytkowników i wykorzystującego możliwości nowych technologii – w celu dostawy szeroko rozumianych usług publicznych o wystarczająco wysokiej jakości, realizowanych szybciej, efektywniej oraz w sposób bezpieczny i niezawodny.

Z punktu widzenia problematyki bezpieczeństwa warto podkreślić cztery elementy tej definicji: odwołanie do zarządzania miastem (czyli podejmowania decyzji przez władze), zaangażowanie mieszkańców, dostawę usług publicznych (a taką usługą jest zapewnienie bezpieczeństwa użytkownikom miasta) oraz realizację tych usług w sposób bezpieczny i niezawodny. Celowo pomijam w tym miejscu nowe technologie – te w mieście inteligentnym są ważne, jednak pełnią funkcję narzędzia, a nie celu.

Bezpieczeństwo z dwóch perspektyw

Zanim połączymy idee miasta inteligentnego (*smart city*) i miasta bezpiecznego (*safe city*), spójrzmy, jak problem miejskiego bezpieczeństwa postrzegają dwie grupy: eksperci i mieszkańcy. Co mówią eksperci o bezpieczeństwie? Jak wyobrażają sobie bezpieczne miasto? W pierwszej kolejności wspominają o gotowości na poważne zagrożenia, takie jak katastrofy komunikacyjne lub naturalne, epidemie, terroryzm i cyberterroryzm czy związane z imprezami masowymi. Mieszkańcy postrzegają problem bezpieczeństwa zupełnie inaczej. Co ich interesuje? (Nie)bezpieczne przejścia dla pieszych, zagrożenia związane z parkowaniem samochodów na chodnikach, piraci drogowi, ciemne i nieoświetlone zaułki, jakość powietrza, drobne włamania i kradzieże – a więc kwestie, które wielu profesjonalistów z branży security traktuje jako co najwyżej drobne uciążliwości. Z czego wynika takie podejście mieszkańców? Oczywiście z doświadczenia. Te „drobne uciążliwości” są codziennością większości tych, któ-



T E K S T
Bartosz Dominiak

rzy korzystają z miasta w stopniu wykraczającym poza przejazd samochodem z garażu podziemnego w domu do garażu podziemnego w miejscu pracy czy galerii handlowej. W pewnym stopniu jest podobnie, gdy popatrzymy na statystyki policyjne w średnim mieście w Polsce. Trudno w nich szukać dużej liczby osób poszkodowanych w zamachach terrorystycznych czy choćby w imprezach masowych. Za to poszkodowanych w wypadkach drogowych jest sporo. Podobne wyniki przyniesie kwerenda w gazetach lub portalach piszących o sprawach lokalnych.

Miasto inteligentnie bezpieczne

Czy to oznacza, że eksperci się mylą? Czy spojrzenia profesjonalistów i mieszkańców są ze sobą sprzeczne? Dwa razy „nie”. Podejście osób zawodowo zajmujących się analizowaniem bezpieczeństwa w miastach uwzględnia zupełnie inny poziom wiedzy i doświadczenia niż w przypadku codziennych użytkowników. Mamy tutaj dwie różne perspektywy, które warto łączyć, by uzyskać efekt synergii. Wróćmy do zarysowanej na początku definicji miasta inteligentnego. Zarządzanie współczesnym miastem oznacza m.in. podejmowanie decyzji opartych na danych i wiedzy, nie na intuicji. Takie podejście wymaga wspar-

Podejście osób zawodowo zajmujących się bezpieczeństwem w miastach uwzględnia zupełnie inny poziom wiedzy i doświadczenia niż mieszkańcy



Czy dwa podejścia do zarządzania – ekspertów i mieszkańców – oparte na wiedzy i zaangażowaniu można połączyć przy ustalaniu priorytetów miejskiej polityki bezpieczeństwa?

➔ cia ekspertów od bezpieczeństwa. Jednocześnie miasto inteligentne musi angażować możliwie największą liczbę swoich użytkowników. A to oznacza, że przy formułowaniu swoich polityk nie może ignorować głosu mieszkańców w tak istotnej kwestii, jaką jest bezpieczeństwo.

Czy te dwa podejścia do zarządzania – ekspertów i mieszkańców, oparte na wiedzy i zaangażowaniu mieszkańców – można połączyć przy ustalaniu priorytetów miejskiej polityki bezpieczeństwa? Jest to możliwe, jeśli zaczniemy myśleć o bezpiecznym mieście jako o takim, które jest gotowe chronić swoich użytkowników przed poważnymi zagrożeniami, a przy tym na co dzień nie zapomina o drobnych uciążliwościach (ale poważnych dla jednostek). Miasto postępujące w tym duchu określam jako miasto inteligentnie bezpieczne.

Transformacja w sześciu krokach

Na koniec spróbuję odpowiedzieć na jeszcze jedno pytanie: jakie działania pozwalają dokonać transformacji miasta w miasto inteligentnie bezpieczne? Chociaż każde miasto jest inne, można wskazać kilka obszarów sprzyjających takiej transformacji. Po pierwsze, kluczowym wyzwaniem jest holistyczne podejście do zarządzania wyzwaniami związanymi z bezpieczeństwem. Nie można traktować poszczególnych obszarów bezpieczeństwa, definiowanych w odmienny sposób przez ekspertów i mieszkańców, w oderwaniu od pozostałych. Definiując działania miasta w tym zakresie, łączmy bezpieczeństwo fizyczne, zdrowotne, ekonomiczne, ekologiczne, cybernetyczne czy socjalne.

Po drugie, trudno zarządzać inteligentnym bezpieczeństwem w mieście, którego organizacja opiera się na podejściu branżowym. Trzeba szukać sposobów na przełamywanie „silosów” departamentów i biur na rzecz zastępowania ich podejściem projektowym z wykorzystaniem zespołów multidyscyplinarnych. Projektując monitoring wizyjny, zaprosimy do współpracy nie tylko ekspertów od kamer, oprogramowania i infrastruktury miejskiej, ale także przedstawicieli ochrony środowiska, transportu publicznego czy komunikacji społecznej. Efekty mogą być zaskakujące.

Po trzecie, konieczne jest tworzenie mechanizmów stałego dialogu z użytkownikami miasta. To oni wiedzą najlepiej, w jakim mieście czują się bezpiecznie, a jakie jawi im się groźne. Tego głosu nie tylko warto słuchać w trakcie bezpośrednich, okazjonalnych dyskusji (np. w ramach konsultacji społecznych), ale także wyciągać wnioski ze zgłoszeń interwencyjnych mieszkańców, np. w ramach takich projektów, jak Warszawa 19115. Po czwarte, miasto inteligentnie bezpieczne musi reagować na drobne wykroczenia. W pewnym stopniu można tutaj doszukiwać się odwołania do idei „zero tolerancji” rozpowszechnionej przez burmistrza Giulianiego w Nowym Jorku w latach

90. ub. wieku. Ale jest subtelna różnica – Giuliani budował wizerunek silnej i bezwzględnej władzy, często za pomocą policyjnej pałki i mandatów. W *smart city* też chodzi o reagowanie na pozornie niewielkie naruszenia prawa, często powszechnie tolerowane i usprawiedliwiane, np. parkowanie na trawnikach i w innych miejscach do tego nieprzeznaczonych, jazda bez biletu autobusem czy brak segregowania odpadów komunalnych. Ale miasto inteligentne poszukuje rozwiązań dla takich postaw w odpowiednim planowaniu infrastruktury i wykorzystaniu technologii.

Po piąte, miasto inteligentnie bezpieczne musi być przygotowane na poważne zagrożenia zarówno z przyczyn naturalnych, jak i np. działań terrorystycznych. Dlatego ważnym zadaniem jest budowa skutecznego, efektywnego i zintegrowanego systemu reagowania na kryzysy, obejmującego nowoczesne centrum zarządzania kryzysowego integrujące pracę wszystkich służb, przemyślane i przećwiczone procedury, zaplanowaną logistykę w przypadku wystąpienia zagrożeń, ciągłą edukację mieszkańców. Po szóste, u progu trzeciej dekady XXI w. żadne miasto inteligentne nie może pomijać nowoczesnych technologii. I nie chodzi tutaj o technologie oraz nowoczesność same w sobie. Należy poszukiwać rozwiązań adekwatnych do potrzeb. Czasami dany problem można rozwiązać bez kosztownych inwestycji w nowoczesny i zaawansowany sprzęt – wystarczą dobry pomysł, drobne zmiany w infrastrukturze, procedurach lub organizacji. Dlatego, wracając do pierwszych trzech punktów, warto patrzeć na bezpieczeństwo kompleksowo, unikając „silosów” i uważnie wsłuchując się w głos użytkowników miasta. Przy takim podejściu można znaleźć rozwiązania nieoczywiste, ale skuteczne. ▢

Niniejszy artykuł jest rozwinięciem prezentacji, przedstawionej przez autora podczas Security Forum Bezpieczne Miasto 2020, które odbyło się 27 lutego 2020 r. w Warszawie.

B I O

Bartosz Dominiak

Autor jest zastępcą burmistrza dzielnicy Ursynów m.st. Warszawy. Od lat zajmuje się problematyką rozwoju miast inteligentnych w Polsce. Prowadzi zajęcia ze studentami w ramach przedmiotów poruszających tematykę *smart city*.

Osiągnięcia Dallmeier w niemieckim sektorze Bezpieczne Miasto



Dla firmy Dallmeier, niemieckiego producenta rozwiązań z zakresu dozoru wizyjnego, ostatnie trzy lata były w sektorze Safe City w Niemczech niezwykle udane. Wynalazca wieloprzetwornikowych kamer Panomera® z systemami rejestracji i oprogramowaniem do analizy i zarządzania sygnałem wizyjnym zrealizował już 19 dużych projektów w niemieckich miastach. Ocena ostatnich incydentów po raz kolejny potwierdziła wysoką skuteczność systemów.

O sukcesie lub porażce stosowania technologii dozoru wizyjnego w przestrzeni publicznej decydują trzy czynniki. Po pierwsze należy zagwarantować wysoką użyteczność obrazu, zwłaszcza maksymalnie spójną, wysoką jakość obrazu w całym rejestrowanym obszarze - to jedyny sposób na zapewnienie możliwości wykorzystania obrazów w sądzie, a przede wszystkim na uzyskanie poprawnego działania algorytmów automatycznej analizy tych obrazów. Po drugie, cel ten powinien zostać osiągnięty przy jak najmniejszej liczbie zastosowanych kamer, aby ogólne koszty, złożoność i obciążenie pracą operatorów utrzymać na niskim poziomie. I wreszcie kluczowe znaczenie ma jakość stosowanego oprogramowania do zarządzania sygnałem wizyjnym oraz algorytmów analizy obrazów na żywo i nagrań.

Minimalna liczba kamer, maksymalne pokrycie

Te trzy elementy łącznie tworzą istotną wartość dodaną opatentowanych systemów kamer wieloprzetwornikowych Panomera®,

Kamera Panomera® zawiera kilka modułów kamerowych, każdy o odpowiedniej ogniskowej obiektywu i czułości przetwornika obrazu, zaprojektowane do obserwacji sceny w różnej odległości od kamery. W rezultacie otrzymujemy jednolity ogólny obraz o takiej samej minimalnej rozdzielczości w całym dozorowanym obszarze.

które Dallmeier wprowadził na rynek w 2011 r. Przełom w sektorze Bezpieczne Miasto nastąpił pod koniec 2016 r. wraz z udanym uruchomieniem takich kamer na Domplatte (plac katedralny) w Kolonii. Policja może tu obserwować obszar prawie 9 tys. m², przy minimalnej gęstości pikselowej 250 pikseli na metr (odpowiednio do normy DIN-EN 62676-4), na którym to obszarze znajduje się tylko 8 kamer Panomera®. Taka właśnie gęstość pikselowa jest wymagana, aby móc identyfikować osoby. Dzięki dużym instalacjom w 19 niemieckich miastach, m.in. we Frankfurcie, w Essen, Chemnitz i w Bremie, producent może poszczycić się doskonałymi osiągnięciami w dziedzinie monitoringu miejskiego.

– Od 2018 r. z wielkim powodzeniem stosujemy technologię Dallmeier Panomera®. Szczególne korzyści czerpiemy z faktu, że podgląd całego obszaru jest zawsze utrzymywany, dzięki czemu operatorzy mogą powiększać dowolne fragmenty z wysoką rozdzielczością nawet podczas nagrywania – mówi Thorsten Wünschmann, szef Urzędu Porząd-

ku Publicznego w Hanau. – W ten sposób zapewniamy optymalną kontrolę przy minimalnym nakładzie pracy operatora, a dzięki temu, że potrzeba tylko kilku systemów, osiągamy również niski całkowity koszt posiadania – dodaje.

Ochrona danych jako rzecz oczywista

Ważnym aspektem akceptacji rynkowej jest również ochrona danych osobowych. Firma Dallmeier spełnia ten wymóg, ściśle przestrzegając wytycznych RODO, „Privacy by Design” i „Security by Design”. Dallmeier projektuje i produkuje wszystkie istotne komponenty rozwiązań w swojej siedzibie głównej w Niemczech, korzysta z usług zewnętrznych firm prowadzących szeroko zakrojone testy penetracyjne i bezpieczeństwa oraz oferuje klientom obszerną dokumentację i wsparcie przy wdrażaniu rozwiązań z zakresu bezpieczeństwa systemów wizyjnych, zgodnych z przepisami o ochronie danych. ▢

Więcej informacji:
Dallmeier Safe City Solutions
<https://www.dallmeier.com/solutions/safe-city>

Dallmeier electronic

Bahnhofstr. 16,
93047 Regensburg
Niemcy
www.dallmeier.com





Miejski wymiar bezpieczeństwa

Krótką analiza Rankingu Dzielnic 2020

Lokalny wymiar zagrożeń w istotny sposób wpływa na poczucie bezpieczeństwa mieszkańców. Realny poziom przestępczości i innych społecznie nieakceptowanych zachowań jest konfrontowany z głęboko uświadomionymi potrzebami pewności, spokoju, redukcji zagrożeń głównie w miejscu zamieszkania, tam gdzie dorastają nasze dzieci, gdzie realizujemy ważne aktywności pozazawodowe. Policja i inne instytucje, m.in. profesjonalne ośrodki badania opinii, analizują sytuację związaną z przestępczością, metodami działania sprawców, ze stopniem pokrzywdzenia ofiar oraz z faktycznymi i społecznymi kosztami czynów zabronionych.



T E K S T

Rafał Batkowski

Jednym z najważniejszych elementów, badanych w kontekście identyfikowanych zagrożeń, jest społeczne poczucie bezpieczeństwa. W roku 2020 na zlecenie Otodom Agencja Badawcza IQS zadała pytania ponad 120 tys. mieszkańców 12 miast Polski: Białegostoku, Bydgoszczy, Gdyni, Gdańska, Katowic, Krakowa, Lublina, Łodzi, Poznania, Szczecina, Warszawy i Wrocławia w celu dokonania oceny różnych aspektów życia w swojej okolicy¹. Respondenci, oceniając bezpieczeństwo, korzystali z pięciopunktowej skali od 1 do 5 (5 było najwyższą, pozytywną notą). Badani odnosili się m.in. do następujących stwierdzeń:

- W mojej dzielnicy czuję się bezpiecznie. Nie boję się po niej poruszać ani wracać do domu po zmroku.
- Według mnie moje dziecko jest bezpieczne poza domem w tej dzielnicy.

Inicjatywa Otodom wpisuje się w wiele innych prób przedstawiania rzetelnego obrazu zagrożeń w miastach, podejmowanych przez władze samorządowe, korporacje poszukujące

1) Druga edycja Rankingu Dzielnic Otodom, na podstawie badania ilościowego zrealizowanego przy użyciu standaryzowanego kwestionariusza za pomocą metodologii CAWI (ang. Computer-Assisted Web Interview) – wspomagany komputerowo wywiad za pomocą strony internetowej. Źródło: <https://www.otodom.pl/wiadomosci/ranking-dzielnic/> (dostęp: 25.05.2020).



Pracownia badawcza zapytała tysiące mieszkańców Warszawy, która dzielnica stolicy ich zdaniem jest najbardziej bezpieczna, a w której nie czują się zbyt dobrze. Analiza odpowiedzi pozwala stwierdzić, że w Warszawie mieszkańcy czują się bezpiecznie. Zanotowano niewielkie różnice pomiędzy dzielnicami wskazywanymi jako najbezpieczniejsze w porównaniu z innymi.

WARSZAWIACY ocenili, że najmniej bezpiecznymi dzielnicami stolicy są:

1. Praga-Północ (3,45)
2. Śródmieście (3,53)
3. Ochota (3,66)
4. Targówek (3,69)
5. Włochy (3,69)

Zwyciężył Wilanów z notą 4,28².

Zdziwienie budzi obecność Śródmieścia wśród niepewnych lokalizacji. W poprzedniej edycji rankingu Otodom z 2017 r. Śródmieście klasyfikowano jako bezpieczną dzielnicę – obecnie na przedostatnim miejscu, co może wymagać dalszych badań.



SZCZECIN w badaniach Otodom zawsze wyróżniał się pozytywnie wśród innych polskich miast. Obecnie zajmuje wysokie miejsce pod względem bezpieczeństwa mieszkańców – z oceną 3,85. Wydaje się, że im dalej od centrum, tym jest lepiej, co potwierdzają noty trzech dzielnic, które szczególnie zapracowały na wiele pozytywnych opinii mieszkańców. Inne rejony miasta lepiej unikać po zmroku, m.in.

1. Śródmieście-Zachód (3,36)
2. Żydowce-Kłucz (3,37)
3. Turzyn (3,41)
4. Pomorzany (3,44)
5. Drzetowo-Grabowo (3,47)

Najlepiej oceniono bezpieczeństwo w dzielnicy Warszawa (4,41)³.

2) Źródło: <https://www.otodom.pl/wiadomosci/ranking-dzielnic/najbezpieczniejsza-dzielnica-warszawy-od-lat-ta-sama-id9756.html> (dostęp: 25.05.2020).

3) Źródło: <https://www.otodom.pl/wiadomosci/ranking-dzielnic/szczecin-jednym-z-najbezpieczniejszych-miast-polski-id9755.html> (dostęp: 25.05.2020).

miejsz na inwestycje, firmy lokujące swoje przedstawicielstwa czy deweloperów, a szerzej mówiąc, branżę nieruchomości. To wartościowe, nowoczesne podejście, które powinno implikować troskę władz o każdy aspekt bezpieczeństwa miasta. Wydaje się jednak, że subiektywne poczucie bezpieczeństwa obywateli, prezentowane w badaniach, powinno zostać skonfrontowane z obiektywnym stanem przestępczości w wybranych obszarach miejskich. Kierowanie się jedynie opinią mieszkańców w materiale Otodom podsumowującym badania, mimo że to bardzo istotny element oceny, nie odzwierciedla rzeczywistego obrazu bezpieczeństwa dzielnic. W związku z tym decyzje o nowych inwestycjach, lokalizacjach siedzib podmiotów gospodarczych lub osiedli czy też prowadzeniu zawodowej aktywności powinny zostać poprzedzone szerszą analizą środowiska bezpieczeństwa.

Warto zapoznać się z wartościowymi badaniami Otodom w całości. Na potrzeby niniejszego krótkiego artykułu koncentrujemy się na Warszawie, Szczecinie i Poznaniu.

Statystyki policyjne

Na podstawie danych, które prezentuje policja, można określić stan zagrożeń bliski rzeczywistości. W 2019 r. zanotowano 760 447 przestępstw – mniej o 8689, tj. o 1,1% w porównaniu do roku 2018, co jest niewątpliwie sukcesem i podtrzymaniem wieloletniego trendu spadkowego (ujmując problem generalnie). Przy tak identyfikowanym stanie zagrożeń należy zauważyć wysoką wykrywalność, na poziomie 72% (wzrost o 0,4%). Niestety są także niepokojące wzrosty liczby przestępstw w kilku kategoriach, m.in. kradzież, rozbój z bronią lub innym narzędziem, czyny zabronione z ustawy o przeciwdziałaniu narkomanii, oszustwo gospodarcze. Notujemy także, niestety, wzrost zagrożenia na naszych drogach, tj. więcej wypadków i ofiar śmiertelnych. W wymiarze regionalnym nieco większe zagrożenie w porównaniu do 2018 r. identyfikujemy w województwach: podlaskim, lubuskim, zachodniopomorskim, śląskim i świętokrzyskim. Pandemia SARS-CoV-2 ograniczyła znacząco przestępczość w tradycyjnym rozumieniu tych zjawisk społecz-



POZNAŃ przez mieszkańców wysoko oceniany i nagradzany za jakość życia, inwestycje miejskie i prospołeczny charakter sprawowania władzy. W rankingu Otodom zaskakują więc nie najlepsze noty Poznania – średnia ocena to 3,78, co plasuje miasto w połowie stawki wśród 12 miejscowości, dla których przygotowano Ranking Dzielnic 2020. Najlepiej wypadły Lublin (3,92), Białystok i Gdańsk (po 3,91). Najmniej bezpiecznie czują się mieszkańcy Łodzi, którzy wystawili miastu ocenę 3,43.

Mieszkańcy Poznania najmniej bezpiecznie czują się w następujących dzielnicach:

1. Główna (3,19)
2. Stare Miasto (3,41)
3. Ostrów Tumski-Śródka (3,43)
4. Wilda (3,52)
5. Morasko (3,54)⁴

Wydaje się, że najbezpieczniej w opinii respondentów jest w dzielnicy Łacina (4,21).

1. Bezpieczeństwo cyfrowe
2. Bezpieczeństwo zdrowotne
3. Bezpieczeństwo infrastrukturalne
4. Bezpieczeństwo osobiste mieszkańców

Doceniając Ranking Dzielnic Otodom – badanie realizowane na znaczącej, należy sądzić, że reprezentatywnej grupie respondentów – trzeba zauważyć potencjalny wpływ tego badania na budowanie opinii o polskich miastach. Mając jednak na uwadze inne źródła danych, ukazujące często odmienny obraz bezpieczeństwa, powinniśmy zmierzać do maksymalnej obiektywizacji badań z wykorzystaniem m.in. statystyk policyjno-prokuratorskich. Dostęp do narzędzi stosowanych w międzynarodowych analizach może pozwolić na wygenerowanie informacji istotnych dla miejskiego samorządu w celu podejmowania działań doskonalących. Przyjęcie takiej perspektywy jest szansą na prezentowanie naszych miast w międzynarodowych rankingach, a co za tym idzie osiągnięcie przewagi w konkurencji m.in. o turystów, studentów i inwestycje. Konsekwencją takiego podejścia może być myślenie o miejskiej marce rozpoznawanej globalnie, także w perspektywie bezpiecznych przestrzeni dla mieszkańców i inwestorów, co powinno być elementem miejskiej strategii. □

R E K L A M A

B I O

dr Rafał Batkowski

Inspektor policji w stanie spoczynku (służba w latach 1993 – 2017, w tym m.in.: naczelnik Zarządu Operacji Antyterrorystycznych w KGP, zastępca dyrektora Biura Prewencji i Ruchu Drogowego KGP, mazowiecki i wielkopolski komendant wojewódzkiej policji oraz dyrektor Biura Międzynarodowej Współpracy Policji KGP, szef Krajowego Biura Interpolu i członek Zarządu Europolu). Prezes Zarządu w Stowarzyszeniu Ekspertów Bezpieczeństwa RP. Właściciel firmy RBS. Obecnie Honorowy Prezes SEB RP. Wykładowca akademicki, autor wielu publikacji z dziedziny bezpieczeństwa publicznego, m.in. w odniesieniu do przeciwdziałania poważnym zagrożeniom, w tym terroryzmowi oraz lokalnego wymiaru bezpieczeństwa i współpracy policji ze społeczeństwem.

nych, przede wszystkim zdarzenia występujące w przestrzeni publicznej. Jednocześnie można zauważyć aktywizację sprawców w sferze cyfrowej – oszustwa, wyłudzenia internetowe, telefoniczne itd. Pełny obraz zagrożeń związanych z epidemią będzie dostępny w kolejnych miesiącach i powinien być przedmiotem precyzyjnych analiz.

Odnosząc się ponownie do wyżej prezentowanych badań Otodom dotyczących Warszawy, Szczecina i Poznania, należy je zestawiać z kilkoma danymi obiektywnymi nt. liczby przestępstw⁵. Warszawa ma prawie 1 mln 800 tys. mieszkańców, co przy liczbie przestępstw ponad 51,6 tys. w 2019 r. daje wskaźnik zagrożenia przestępczością na 100 tys. mieszkańców na poziomie 2919,8. Taki stan kontroli przestępczości ukazuje stolicę kraju, dużą aglomerację, w dobrym świetle i koresponduje (generalnie) z ustaleniami badaczy działających na zlecenie Otodom. Szczecin z liczbą ponad 400 tys. mieszkańców i przestępczością na poziomie prawie 23 tys. zdarzeń osiąga wskaźnik 5694,4 na 100 tys. mieszkańców. To najgorszy wynik w kraju – zgoła inny obraz w zestawieniu z oceną Otodom. W Poznaniu, mieście liczącym ponad 540 tys. mieszkańców, w roku minionym odnotowano ponad 14,5 tys. przestępstw, co pozwala określić wskaźnik zagrożenia na poziomie 2687,8. To dobry wynik, potwierdzający skuteczną kontrolę przestępczości w mieście. Otodom, opierając się na rankingu dzielnic, prezentuje Poznań w nieco gorszym świetle.

Zmierzając do podsumowania, należy wskazać na dosyć złożoną materię dotyczącą analizowania przestępczości i poczucia bezpieczeństwa mieszkańców na danym terenie. Oprócz kwestii kwalifikacji prawnej konkretnych czynów zabronionych, stanu prowadzonych postępowań przygotowawczych (dane wiążące się z postępowaniami

wszczętymi lub przestępstwami stwierdzonymi), niepełnych danych dotyczących naruszeń stypizowanych w kodeksie wykroczeń, należy również pamiętać o ciemnej liczbie przestępstw (zdarzenia nieujawnione organom ścigania lub organom ochrony prawnej), która zaburza precyzyjny obraz środowiska miejskiego. Ponadto wzrosty liczb bezwzględnych w kilku kategoriach, np. przestępstwa narkotykowe, korupcyjne, gospodarcze, są często wynikiem większego zaangażowania policji – większej „ujawnialności” zdarzeń, o których zwykle ani sprawca, ani ofiara nie mają ochoty informować. Na problemy w analizie porównawczej stanu przestępczości mają wpływ także zmiany w prawie karnym, np. ostatnio problematyka ścigania osób uchylających się od świadczenia alimentów.

Podsumowanie

Dążąc do optymalizacji działań analitycznych oceniających poziom bezpieczeństwa miast, warto też zwrócić uwagę na uznane w wymiarze międzynarodowym badania zagrożeń w aglomeracjach miejskich. Dla przykładu, na podstawie Safe Cities Index 2019 można wskazać najbezpieczniejsze miasta na świecie⁶ – niestety w tym zestawieniu nie znajdziemy polskich:

- | | |
|--------------|---------------|
| 1. Tokio | 6. Toronto |
| 2. Singapur | 7. Waszyngton |
| 3. Osaka | 8. Kopenhaga |
| 4. Amsterdam | 9. Seul |
| 5. Sydney | 10. Melbourne |

Istotnymi kwestiami, w artykule jedynie sygnalizowanymi, są kryteria i metodologia stosowane przez badaczy. Autorzy analizują czynniki wewnętrzne i zewnętrzne w 4 głównych obszarach stanowiących następnie filary oceny sytuacji w miastach:

4) Źródło: <https://www.otodom.pl/wiadomosci/ranking-dzielnic/bezpieczniejak-na-lacinie-id9754.html> (dostęp: 25.05.2020).

5) Średni wskaźnik dotyczący miast wojewódzkich, w których mieszka łącznie ponad 7,5 mln ludzi, wynosi 2899,1, liczba przestępstw oscyluje wokół 220 tys.

6) Źródło: <https://safecities.economist.com/safe-cities-index-2019/> (dostęp: 25.05.2020).



VIDEO INFORMATION TECHNOLOGY for the 21st Century

Learn more: dallmeier.com

Obejrzyj
teraz
video!





SMART CITY
SAFE CITY

NA KOZŁÓWCE – osiedle chronione jak miasto



Jak zapewnić bezpieczeństwo na rozległym i nieogrodzonym osiedlu o powierzchni ok. 180 tys. m², w którym mieszka blisko 10 tys. mieszkańców? Czy ogrodzenie jest elementem koniecznym, aby osiedle było bezpiecznie?

– Ogrodzenie jest co prawda niezaprzeczalne, patrząc na bezpieczeństwo małych dzieci w niewielkich osiedlach, ale w przypadku dużych osiedli, z punktu widzenia wandalizmu i kradzieży, nie odgrywa większej roli – twierdzi Marcin Gromko, menedżer ds. usług wideo w Securitas Polska. Krakowskie Osiedle Mieszkaniowe Na Kozłowie powstało na przełomie lat 60. i 70. i nie zawsze było miejscem tak bezpiecznym jak teraz.

– Wyzwanie, jakie podjęliśmy, przejmując ochronę tego obszaru, polegało głównie na zaklasyfikowaniu go jako kompleks miejski. Zdecydowała o tym złożoność terenu, bardzo duża powierzchnia i liczba mieszkańców – dodaje menedżer. Osiedle Na Kozłowie to kompleks obiektów z pełnym spektrum zagrożeń charakterystycznych dla powierzchni miejskich. Do 2008 r. były to włamania i kradzieże, rozboje, akty wandalizmu, za-

klócanie porządku, pożary, awarie zasilania, zanieczyszczanie, spożywanie alkoholu czy zażywanie narkotyków.

– Nasze doświadczenie jednoznacznie wskazuje, że o skuteczności ochrony decyduje właściwe połączenie różnych usług w tzw. Solutions, rozumiane jako rozwiązanie dedykowane dla konkretnego klienta, łączące kilka usług lub produktów. W przypadku tego osiedla (i podobnych), opracowaliśmy rozwiązanie, które obecnie, z perspektywy kilku lat, możemy wiarygodnie ocenić – tłumaczy M. Gromko.

– Rozwiązania, które zaproponowała nam firma Securitas, nie tylko znacznie podniosły poziom bezpieczeństwa i ograniczyły niepożądane zdarzenia prawie o 50%, ale również zwiększyły komfort życia mieszkańców. Nasze osiedle nie zasypia wraz z nastaniem ciszy nocnej. Mimo że forma prawna określa nas jako osiedle, funkcjonujemy jak małe miasteczko – mówi Radosław Gruszka, prezes Zarządu Spółdzielni Mieszkaniowej Na Kozłowie w Krakowie.

Osiedle Na Kozłowie w liczbach: około 180 tys. m² powierzchni, blisko 10 tys. mieszkańców, ok. 50 budynków mieszkalnych, w tym kilka wieżowców skupiających kilka tysięcy mieszkańców, basen, pawilony handlowo-usługowe, dwie szkoły, dwa przedszkola, żłobek, ośrodek zdrowia, targowisko, apteka, poczta, kawiarnie, puby, placówki bankowe i wiele innych obiektów. Operatorzy mają do dyspozycji kilkaset kamer, które nie naruszają prywatności mieszkańców osiedla, a dozorem obejmują wszystkie niewrażliwe miejsca. Niezwykle ważną okazała się też bezpośrednia współpraca z klientem, który kieruje uwagę Securitas na obszary szczególnie narażone na wystą-

pienie zagrożenia. Kamery pracują w trybie dzień/noc, są wyposażone w czujniki detekcji ruchu, większość obszaru osiedla jest stale oświetlona.

Czynnikiem, który znacznie podniósł poziom bezpieczeństwa, było wprowadzenie komunikacji głosowej z osiedlem. Jeżeli operator widzi na obrazie z kamery zdarzenie wymagające interwencji, przekazuje za pomocą głośników komunikaty głosowe. W przypadku niezastosowania się do poleceń, informuje o interwencji patrolu.

Skuteczność rozwiązania jest bardzo wysoka, w ponad połowie przypadków intruz odstępuje od działania. Operatorzy mogą też w razie konieczności wezwać służby ratunkowe. Prawdopodobieństwo wystąpienia zdarzeń niepożądanych jest skutecznie zredukowane także poprzez stacjonowanie patrolu Securitas na terenie osiedla, przejazdy prewencyjne, cykliczne sprawdzanie miejsc niewrażliwych i spotkania z przedstawicielami klienta oraz straży miejskiej i policji.

– Dbamy również o komfort mieszkańców osiedla. Przygotowujemy dla nich cykliczne porady nt. bezpieczeństwa, uruchomiliśmy specjalny numer alarmowy i adres e-mail, a mieszkańcy coraz częściej korzystają z tych kanałów komunikacji, z czego bardzo się cieszymy – konkluduje Marcin Gromko. □

**Securitas
Polska**

Postępu 6
02-676 Warszawa
securitas@securitas.pl



AS
ALNET
SYSTEMS

**Polskie profesjonalne
zintegrowane rozwiązania
VMS**

**Ponad 200 000 instalacji
na całym świecie
Jesteśmy z Wami od
2003 roku**

Z naszych rozwiązań korzysta

mediaexpert

Lider handlu detalicznego
marek branży RTV-AGD-Multimedia
w Polsce

www.alnetsystems.com



ODPADY POD E-KONTROLĄ →

Problem z nieefektywną segregacją odpadów w zabudowie wielorodzinnej jest jednym z największych wyzwań stojących przed samorządami w Polsce. Wiele z nich wdraża już rozwiązania, które przynoszą oszczędności środków przeznaczanych na ich przetwarzanie.

Włodarze miasta Ciechanów wprowadzili pilotażowo system mający nie tylko zapewniać wymierne korzyści finansowe osobom segregującym śmieci, ale także zachęcać inne samorządy do poszukiwania analogicznych koncepcji.

W roku 2019 w Ciechanowie uruchomiono pilotażowo system segregacji odpadów oparty na inteligentnych kontenerach. Urządzenia te ważą otrzymane worki z odpadami (wcześniej oznaczone naklejkami z indywidualnymi kodami kreskowymi gospodarstw domowych), wysyłają informację na ten temat do systemu centralnego i identyfikują osoby wrzucające śmieci. Rozwiązanie to ma na celu podniesienie świadomości ekologicznej mieszkańców oraz zapewnienie skuteczności recyklingu odpadów (obecnie Polska przetwarza zaledwie ok. 30% z nich, w 2035 r. wskaźnik ten ma wynieść 65%).

Szczegółowy opis rozwiązania

Testy rozpoczęto 11 maja 2019 r. na osiedlu „Płońska” w Ciechanowie. Wzięło w nich udział 336 gospodarstw domowych. Na terenie osiedla rozstawiono specjalnie oznaczone inteli-

gentne pojemniki (każdy o pojemności 1100 litrów) wyposażone w czujniki, których zadaniem jest zważenie otrzymanego worka z odpadami. Aby otworzyć pojemnik, osoba chcąc wrzucić śmieci musi zeskanować kod z naklejki, którą wcześniej otrzymała i oznaczyła nią worek. W ten sposób system nie tylko identyfikuje osobę wrzucającą odpady, ale także może sumować wyrzucane odpady w danym okresie. Dzięki temu jego obsługa może określić, czy osoba wyrzucająca śmieci segreguje je we właściwy sposób, a w wypadku gdyby tak nie było, skontaktować się z nią. Właściwe segregowanie odpadów przekłada się na niższe opłaty.

Pojemników nie można otworzyć bez użycia kodu, co wyklucza wrzucanie śmieci przez osoby do tego nieuprawnione. Pojemniki są nie tylko szczelne, że nie wydobywa się z nich nieprzyjemny zapach ani nie wchodzi do nich gryzonie czy insekty. Koncepcja zastosowana w Ciechanowie zakończyła się sukcesem. Prezydent miasta zadeklarował chęć kontynuowania i rozwijania projektu także na pozostałych osiedlach. Ciechanowskie wdrożenie zainspirowało samorządy w całym kraju. Implementacja podobnego rozwiązania rozważana jest w Chojnicach, a także Olsztynie. ▣



PROBLEM

- Demotywuująca struktura dotychczasowego systemu opłat za segregację odpadów (segregujący i niesegregujący płacili taką samą stawkę)
- Niska skuteczność recyklingu odpadów w Polsce (przetworzeniu poddawane jest ok. 30% śmieci)
- Niska świadomość ekologiczna odbiorców (blisko 65% mieszkańców osiedla przed programem nie segregowało śmieci)
- Odpady wysypujące się z kontenerów zanieczyszczające otoczenie i powodujące nieprzyjemny zapach



KORZYŚCI

- Przezroczystość nowego systemu (osoby segregujące śmieci płacą 13 zł w skali miesiąca za wywóz odpadów, a niesegregujące – aż 25 zł)
- Brak konieczności zadłużania się przez miasto (urządzenia w ramach pilotażu zostały dostarczone przez partnera prywatnego)
- Zwiększenie efektywności recyklingu odpadów (przed pilotażem blisko 65% biorących udział w nim nie segregowało śmieci, po pilotażu tylko 10%)
- Promocja miasta jako pioniera w zakresie inteligentnych rozwiązań w gospodarce odpadami¹³
- Zwiększenie świadomości mieszkańców w kwestii segregacji śmieci (system przynosi korzyści finansowe mieszkańcom tylko wtedy, gdy wszyscy w niego korzystają)
- Poprawa wrażeń estetycznych (dzięki szczelności kontenerów śmieci nie wydostają się na zewnątrz)



REKOMENDACJE

- Objęcie pilotażem możliwie dużej liczby osiedli w celu uzyskania wiarygodnych wyników dotyczących odsetka segregujących
- Przeprowadzenie kampanii informacyjnej wśród mieszkańców na temat korzyści wynikających z segregowania śmieci
- Maksymalna indywidualizacja opłat (powiązanie wysokości opłat z wagą wyrzucanych odpadów)
- Prowadzenie regularnych ankiet wśród mieszkańców w celu zbadania ich preferencji w zakresie segregacji
- Wprowadzenie ułatwień dla seniorów (lekkie klapy kontenerów)

Często mamy do czynienia z sytuacjami, w których ktoś deklaruje segregację, a wcale tego nie robi i mimo wszystko płaci mniej. Nowy system pozwoli to zweryfikować i w konsekwencji egzekwować właściwą opłatę bądź wymusić faktyczną segregację, czyli to, na czym najbardziej nam zależy.

Krzysztof Kosiński,
prezydent Ciechanowa



PARKOWANIE POD E-KONTROLĄ →

Stolica Polski od lat boryka się z problemem niskiej efektywności poboru opłat, a także niewystarczającą rotacją pojazdów w strefach płatnego parkowania niestrzeżonego. Problem unikania opłat przybrał w Warszawie skalę nieporównywalną z żadnym innym miastem w kraju.

Jak podaje Zarząd Dróg Miejskich w Warszawie, aż 9 tys. osób dziennie (7,5%) nie uiszczało płatności za postój. Tak duża liczba łamiących prawo nie tylko szkodziła wizerunkowi miasta, ale także stanowiła znaczną wyrwę w budżecie. Aby zwiększyć przychody z płatności za parkowanie oraz poprawić skuteczność w wystawianiu mandatów, Warszawa, jako jedno z pierwszych miast w Europie, wprowadziła system e-kontroli, który ma nie tylko poprawić wskaźniki finansowe samorządu, ale także zmniejszyć biurokrację oraz ułatwić pracę patrolom pieszym.

Koncepcja ta polega na kontroli pojazdów w strefach płatnego parkowania niestrzeżonego (SPPN) przez elektryczne auto z zamontowaną na nim aparaturą identyfikującą otoczenie. Podczas skanowania aparatura przesyła dane rejestracyjne auta do systemu, który automatycznie sprawdza, czy dany pojazd ma opłacony postój. Jeśli nie ma stosownej opłaty, jego kierowca automatycznie otrzymuje wezwanie do zapłaty. To samo miejsce jest sprawdzane dwa razy w krótkim odstępie czasu, aby wyeliminować naliczenie kierowcy mandatu w czasie, gdy udał się, by kupić bilet. W założeniu dwa elektryczne samochody miały mieć efektywność dziesięciu patroli pieszych. Pierwszego dnia e-kontroli system zanotował 603 kierowców, którzy nie zapłacili za parkowanie.

Projekt rozpoczęty 7 stycznia br. został sfinansowany ze środków unijnych oraz budżetu miasta. Jego koszt 1,9 mln zł obejmuje dwa samochody elektryczne, dwa systemy mobilnej kontroli pojazdów, przeszkolenie operatorów systemu e-kontroli oraz jego ewentualne naprawy w okresie 3 lat od rozpoczęcia. Miasto zastrzegło sobie możliwość do-

kupienia trzeciego samochodu, jeśli rozwiązanie będzie przynosiło oczekiwane efekty. Przeprowadzone wcześniej testy wykazały, że projekt był obciążony niewielkim ryzykiem. Jego wyniki podkreśliły dużą efektywność e-kontroli: dwa samochody elektryczne z zamontowaną aparaturą w ciągu 10 minut były w stanie zidentyfikować ok. 260 pojazdów, co kontrolerowi zajmowało 1 godz. Na tak dużym obszarze, jakim dysponuje stolica, patrole były w stanie skontrolować dziennie zaledwie 40% miejsc do tego przeznaczonych, a dzięki nowemu rozwiązaniu każdy parking będzie kontrolowany co najmniej raz dziennie. System e-kontroli automatycznie anonimizuje twarze przechodniów, a także pozostałe tablice rejestracyjne, dzięki czemu dane personalne są anonimowe. System e-kontroli zaczął przynosić pozytywne efekty niemal od razu: po zaledwie dwóch tygodniach wpływy z uiszczanych opłat wzrosły aż o 10%, a cały projekt zwrócił się po 11 dniach działania.

Koncepcja zastosowana w Warszawie jest rozwiązaniem innowacyjnym, bardzo potrzebnym i skutecznym, czego dowodem są trwające konsultacje nad rozszerzeniem programu na kolejne dzielnice. System pozwala zarówno znacznie podnieść efektywność sprawdzania parkingów, jak i ograniczyć konieczność angażowania zasobów ludzkich. ▢



PROBLEM

- Wysoki odsetek osób niepłacących za postój (ok. 7,5%)
- Niska efektywność patroli pieszych (kontrolerzy potrzebują około godziny na sprawdzenie 260 samochodów, samochody e-kontroli – zaledwie 10 minut)
- Niższe od oczekiwanych wpływy z opłat za parkowanie (w 2018 r. dochody z tego tytułu wyniosły tylko 100 mln zł)
- System zachęcający do unikania opłat za parkowanie (mandat za nieopłacenie parkowania wynosił w 2019 r. zaledwie 50 zł)
- Niesłusznie wystawiane mandaty wynikające z jednorazowej kontroli miejsca parkingowego (patrol wystawiał mandat w czasie, gdy kierowca był w drodze do parkometru, by uiścić opłatę)
- Konieczność wkładania mandatów pod wycieraczkę przedniej szyby samochodu (w nowym systemie o opłaceniu biletu poinformuje skan tablicy rejestracyjnej samochodu)



KORZYŚCI

- Ograniczenie biurokracji (system automatycznie wysyła wezwania do zapłaty, bez konieczności ich drukowania)
- Wysoka efektywność rozwiązania (w 10 minut można sprawdzić 260 pojazdów)
- Efektywniejsze wykorzystanie patroli pieszych (mogą wybierać konkretne miejsca wskazane przez system e-kontroli, np. tam gdzie dostępność do skanowanych rejestracji jest ograniczona)
- Wzrost uiszczania opłat o ok. 10%
- Mniejsza liczba pomyłek i odwołań od mandatów wynikająca z dwukrotnej kontroli tego samego miejsca w krótkim odstępie czasu
- Nienaruszanie prywatności (wizerunek kierowców oraz informacje o otoczeniu są automatycznie anonimizowane)
- Kontrola każdego miejsca w strefach płatnego parkowania niestrzeżonego (SPPN) co najmniej raz dziennie
- Elastyczność nowego rozwiązania – w razie awarii jednego z pojazdów system można zamontować na kolejnym

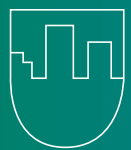


REKOMENDACJE

- Stosowanie systemu w miastach, w których można łatwo skanować duże powierzchnie parkingowe z dużą liczbą aut
- Zharmonizowanie pracy pojazdów i patroli pieszych
- Zaplanowanie tras aut tak, by nie jeździły w trudno dostępne miejsca, gdzie obecność patroli pieszych jest konieczna
- Zróżnicowanie stawek opłat parkingowych zależnie od miejsca i odległości od centrum miasta
- Ograniczanie patroli pieszych (ze względu na ich niską efektywność)

Większa skuteczność kontroli jest w interesie wszystkich warszawiaków. Pieniądze zebrane w strefie trafiają do miejskiej kasy, z której jest m.in. remontowana, modernizowana i budowana infrastruktura drogowa.

Kamil Dąbrowa, były rzecznik prasowy prezydenta m.st. Warszawy



PIERWSZE MIASTO W POLSCE Z DOSTĘPEM DO SIECI 5G →

Włodarze Gdyni podpisali z Play, jednym z operatorów telekomunikacyjnych, memorandum dotyczące dostępu, rozwoju i wdrożenia sieci nowej generacji. Po uzyskaniu odpowiednich zgód formalnych zostanie uruchomiona pierwsza w Polsce sieć 5G obejmująca zasięgiem Gdynię i część Trójmiasta.

Sieć nowej generacji będzie początkowo działać na pasmach obecnie wykorzystywanych na potrzeby telefonii LTE (aukcje na pasma dedykowane nowej technologii dopiero się odbędą) – w Gdyni będzie to pasmo 2100 MHz. Funkcjonowanie sieci 5G w początkowym okresie zwiększy komfort mieszkańców korzystających z mobilnego przesyłu danych. W porównaniu do sieci 4. generacji (LTE) może być to nawet stu-krotne zwiększenie prędkości. Zapewni również większą stabilność funkcjonowania sieci komórkowych, szczególnie na obszarach, gdzie przebywa jednocześnie wiele osób, np. w trakcie imprez masowych.

Główną zaletą wprowadzenia technologii 5G do miast jest możliwość implementacji inteligentnych narzędzi do zarządzania nimi. Parametry techniczne sieci pozwolą m.in. na rozwijanie Internetu Rzeczy (IoT) czy samochodów autonomicznych. Pojawią się też nowe rodzaje aplikacji wykorzystujące potencjał 5G.

Szczegółowy opis rozwiązania

Wprowadzenie sieci 5G jest kluczowa dla idei inteligentnych miast, która została wpisana do strategii rozwoju samorządów. Ta koncepcja jednak ewoluowała. Początkowo „inteligentne miasta” były przede wszystkim etykietą dla ambitnych projektów budowy błyszczącej metropolii na zielonych polach lub pustyni. Gdy te ambitne projekty (m.in. Masdar czy Songdo) zmagają się z dużymi problemami w zakresie rozwoju, na liderów wdrażania idei inteligentnych miast wyrosły inne metropolie: Londyn, Amsterdam czy Singapur, które zamiast odgórnych wizji stworzyły

technologie nazywane platformami inteligentnego miasta. Obecnie miasta aspirujące do miana *smart cities* zakładają, że ich zadaniem jest stworzenie warunków do optymalizacji funkcjonowania, a podstawowy cel stanowi zebranie wszystkich danych o funkcjonowaniu i ich udostępnienie. Ma to pozwolić na stworzenie systemu kontroli i zarządzania w czasie rzeczywistym. Oznacza to, że dane generowane przez miasto będą wykorzystywane do optymalizacji jego funkcjonowania. Przykładem może być połączenie danych pogodowych i transportowych, aby dopasować popyt na taksówki z ich podażą, np. gdy pada deszcz, co kilka lat temu wprowadzono w Singapurze.

Kluczową barierą we wdrażaniu idei inteligentnego miasta była i wciąż jest infrastruktura sieciowa. Dotychczasowa sprawność sieci telekomunikacyjnej (a szczególnie jej przepustowość) nie pozwala na masowe wdrażanie systemów opartych na czujnikach zbierania danych, które są głównym ogniwem IoT. Gdynia, jako pierwsza w Polsce wdrażając technologię 5G, staje się miastem-symbolem rewolucji w zarządzaniu miastem. Najważniejszy aspekt ma charakter promocyjny i reklamowy – miasto ma szansę przyciągnąć projekty pilotażowe i firmy zainteresowane testowaniem swoich rozwiązań, które wymagają nowej technologii. Gdynia zyskuje również rozwiązanie, które szybko może pomóc w usprawnieniu zarządzania miastem, co przyczyni się do zwiększenia atrakcyjności inwestycyjnej samorządu.

Wszystko wskazuje na to, że inteligentne miasta przyszłości nie będą wyglądały inaczej niż obecnie, ale będą działać wydajniej dzięki generowaniu i „rozumieniu” danych. ▢



PROBLEM SIECI 4G

- Technologia uniemożliwiająca rozwój Internetu Rzeczy (IoT)
- Brak wystarczającej ilości danych o funkcjonowaniu miasta
- Fragmentaryczność narzędzi do inteligentnego zarządzania miastem



KORZYŚCI

- Wdrożenie przełomowej technologii w rozwoju miast
- Wykreowanie promocyjnego argumentu w przyciąganiu firm i studentów
- Prowadzenie kampanii informacyjnych, czyli oswojenie mieszkańców z nową technologią, która wywołuje kontrowersje
- Możliwość wdrożenia innowacyjnych rozwiązań z zakresu smart cities, dla których dotychczasowa infrastruktura technologiczna była niewystarczająca
- Szansa przyciągnięcia firm i start-upów, które potrzebują miejsca do testowania swoich rozwiązań



REKOMENDACJE

- Umożliwienie firmom telekomunikacyjnym rozwoju sieci 5G (współpraca w zakresie infrastruktury i promocji)
- Wykorzystanie sieci 5G do zbierania danych o funkcjonowaniu miasta
- Stworzenie platformy do udostępniania danych o mieście – konkretne rozwiązania ich wykorzystania powinny proponować firmy, uczelnie i start-upy
- Promocja technologii 5G jako zmieniającej codzienne funkcjonowanie miasta

To bezprecedensowe partnerstwo z Play pozwoli naszym mieszkańcom na pełne wykorzystanie innowacyjnych rozwiązań oferowanych przez sieć 5G. Dzięki szerokiemu zakresowi współpracy technologia ta będzie dostępna nie tylko w warunkach laboratoryjnych, ale także dla użytkowników indywidualnych, instytucji szkolnictwa wyższego i osób starszych w celu promowania integracji cyfrowej.

Wojciech Szczurek, prezydent Gdyni



W ROKU 2019 OPUBLIKOWALIŚMY SERIĘ ARTYKUŁÓW „DŻUNGLA MIASTA WG JACKA I JACKA” UKAZUJĄCĄ RÓŻNE OBLICZA BEZPIECZEŃSTWA W MIEŚCIE. OBECNIE KONTYNUUJEMY TEN WĄTEK W UJĘCIU BARDZIEJ USYSTEMATYZOWANYM I OPARTYM NA PRZYKŁADACH PROGRAMÓW I STRATEGII W KONKRETNYCH MIASTACH, WRAZ Z NARZĘDZIAMI, TECHNOLOGIAMI I ROZWIĄZANIAMI METODOLOGICZNYMI WSPIERAJĄCYMI TEN PROCES. ZAPRASZAMY DO BANGKOKU.

Przetrwają odporni!

Strategia Bangkoku

CZ. 2

Od kilku lat obserwujemy rozwijający się dynamicznie model analizy i zarządzania miejskim życiem, nazywany odpornością lub terminem angielskojęzycznym *urban resilience*. Odpornością miast zajmowała się w sposób metodyczny m.in. powołana przy Fundacji Rockefellera organizacja 100 Resilient Cities. Obecnie spadkobiercą tej organizacji jest Global Resilient Cities Network. Posługując się opracowanym przez nią narzędziem analitycznym „City Resilient Index”, miasta na całym świecie mogą zbadać swój poziom odporności na różne zagrożenia i wyzwania. Co ciekawe, tradycyjnie postrzegane przez „bezpieczników” zagrożenia kryminalne, terrorystyczne i pochodne ważą w tym rankingu mniej niż wyzwania z obszaru zanieczyszczenia środowiska, dostaw wody i pozostałych mediów, cyberprzestępstw oraz innych wywodzących się wprost z przyrody czy charakteru lub swoistej specjalizacji miast. Odporność miejska staje się również przedmiotem zainteresowania państw i organizacji, np.

ONZ (agenda badawcza UNHABITAT) czy Unia Europejska (projekt TURAS).

W serii artykułów przybliżymy strategię i narzędzia takich miast jak Bangkok, Bristol, Chicago, Rotterdam, Rio de Janeiro. Z krajowego podwórka pokażemy przykład Krakowa, który co prawda nie ma strategii odporności w rozumieniu metodologii „100RC”, ale grupa badawcza z UJ wraz z władzami miasta od lat prowadzi badania nad miejskim bezpieczeństwem. Każde z nich ma własne priorytety odporności wynikające z ich specyfiki i każde buduje indywidualne strategie wypełnienia celów tych strategii.

Jak to robią w Bangkoku

Bangkok, 8-milionowa stolica Tajlandii, z zespołem metropolitalnym przekraczająca 14 mln mieszkańców, jest 40 razy większy niż kolejne co do wielkości miasto w tym kraju. Cała Tajlandia jest najpopularniejszą turystyczną destynacją na świecie. Królestwo bije rekord za rekordem i wg danych w 2019 r. odwiedziło je blisko 40 mln zagranicznych turystów, prawie trzykrotnie więcej niż 10 lat temu. Taki skok jest powodem do zadowolenia, ale również zmartwieniem dla władz. Przychody z turystyki są ogromne, choć jednocześnie istnieje spore zagrożenie, że ten raj na ziemi zostanie zniszczony przez turystów.

Strategia odporności miasta Bangkok została ukierunkowana, a jej ciężar gatunkowy przeniesiono na kwestie środowiskowe. Ma ona trzy zasadnicze obszary działania opar-



T E K S T
Jacek Tyburek

te na wielu ważnych celach wspieranych przez pakiet inicjatyw i projektów. Koncentrują się one na jakości życia oraz ograniczaniu ryzyka. Zwiększenie adaptacji oraz napędzanie gospodarki jej konkurencyjnością stanowi główny cel, którego polityka odporności ma być osłoną. Istotnym wyzwaniem są nowe kreatywne sposoby rozwiązywania podstawowych problemów w mieście, m.in. rozładowania korków w ruchu drogowym i kwestie związane z powodzią.

Poprawa jakości życia w mieście, jako zadanie strategiczne, jest realizowana poprzez uruchomienie programów rozpoznania najpilniejszych potrzeb w zakresie ochrony zdrowia i dobrostanu dla wszystkich mieszkańców miasta (nie tylko Tajów). Zadania planuje się na dziś i na najbliższą przyszłość. Istotną kwestią jest zapewnienie bezpiecznej i dostosowanej do ciągle rosnącego zapotrzebowania korekty systemu dróg. Bangkok powiększa się dynamicznie, wchłaniając kolejne peryferyjne miejscowości. W strategii odporności postawiono wymóg, aby każda korekta granic miasta brała pod uwagę nie tylko potrzeby urbanizacji tych terenów, ale przede wszystkim dbałość o środowisko naturalne.

Powiększające się miasto zlokalizowane nad rzeką musi liczyć się ze stałym zagrożeniem powodziowym. Okresowe powodzie i podnoszenie się stanu wód nie robią obecnie na mieszkańcach większego wrażenia. Dla nich to naturalny cykl życia od wieków. Bangkok to jednak miasto ambitne i podejmuje się wyzwań – ograniczanie ryzyka powodzi poprzez uruchomienie przygotowań od strony infrastrukturalnej, organizacyjnej i technologicznej stanowi obecnie cel działania władz miejskich.

Tajlandia i Bangkok są synonimami azjatyckiego cudu gospodarczego lat 80. i 90. XX wieku. Miasto do swo-



jej strategii rozwoju i odporności wpisuje stałą troskę o ekonomiczną atrakcyjność miasta jako miejsca prowadzenia biznesu. Co oczywiste, szczególną pozycję zajmuje tutaj dążenie do ciągłego rozwoju turystyki, sfery usług turystycznych oraz poprawy jakości pobytu turystów.

Rola ochrony fizycznej oraz projekt cudzoziemskich asystentów policji ds. turystyki

Bangkok to miejsce bezpieczne dla turystów i mieszkańców, ale jednocześnie prześląknięte wszechobecną ochroną fizyczną. Trudno o wiarygodne źródła danych na temat liczby osób zatrudnionych w ochronie. W prasie publikowanej w sieci można znaleźć informacje, że w całej Tajlandii w ochronie znajduje zatrudnienie ok. 400 tys. osób, z czego w Bangkoku ok. 200 tys. Niestety przykrą dla branży informacją jest to, że ludzie ci znajdują się na dole placowej drabiny w Tajlandii. Pracownik ochrony zarabia o ok. 30% mniej niż szeregowy pracownik sektora usług dla turystów. Wypełnia różne funkcje: od prac porządkowych po incydentalne kierowanie ruchem w mieście w kamizelkach policji.

Jednym z ciekawszych przykładów wkładu elementu bezpieczeństwa jako czynnika poprawiającego atrakcyjność turystyczną miasta jest instytucja służby policyjnej FTPA (Foreign Tourist Police Assistants – asystenci policji ds. turystów zagranicznych) złożona z wolontariuszy cudzoziemców. Powodem wdrożenia tego systemu była m.in. bardzo słaba znajomość języków obcych wśród policjantów i pracowników ochrony w całej Tajlandii oraz wynikające stąd nieporozumienia. Cudzoziemscy wolontariusze policyjni patrolują Walking Street już od 2002 r., kiedy to Wydział Turystyki Policji Pattaya zaprosił ich do pomocy. Początkowo ich główną rolą była pomoc miejscowym oficerom w tłumaczeniu i zapewnienie nieformalnych usług informacyjnych turystycznej. FTPA nadal zapewnia wsparcie dla zagranicznych gości, ale jego zakres został poszerzony o obowiązki interwencji, np. w przypadku bójek w barach czy zatrzymywanie złodziei. Choć ochotnicy nie mają uprawnień do aresztowania (wymagana jest zgoda tajlandzkiego oficera nadzorującego), noszą kajdanki, pałki i pojemniki z gazem pieprzowym. Czarnymi mundurami SWAT robią imponujące wrażenie.

FTPA liczy ok. 60 członków z 20 krajów, a jej zasięg wychodzi poza obszar Pattaya dzięki wprowadzeniu patroli motocyklowych. Mimo to Walking Street, którą patrolują co wieczór od 21.00 do 3.00, pozostaje głównym miejscem ich pracy. Dla rzeszy

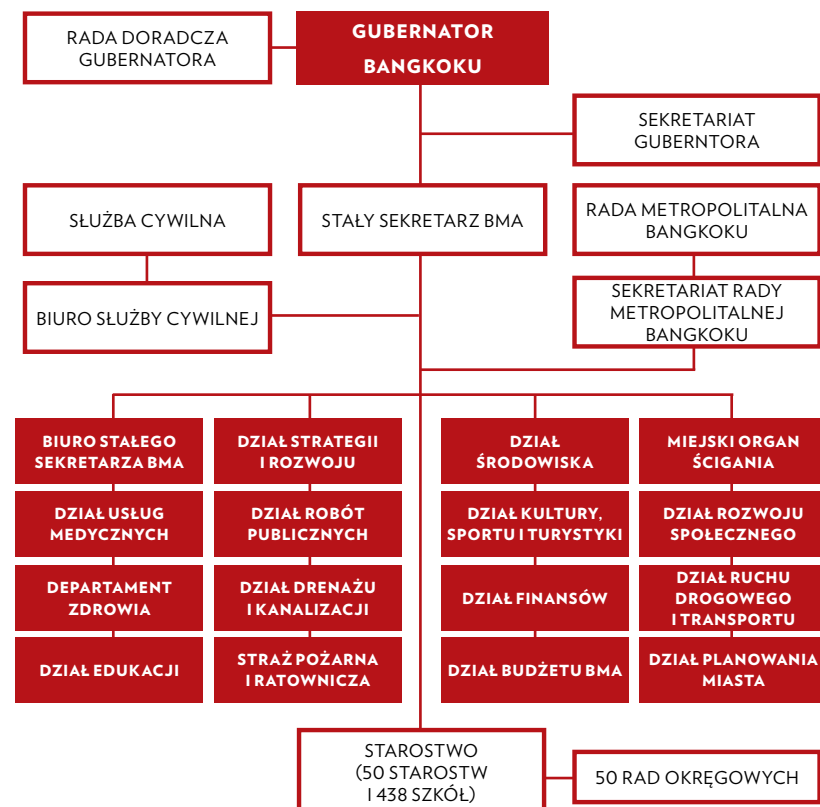
odwiedzających mężczyzn arteria jest celem ich przyjazdu do Tajlandii. Pas dla pieszych rozciągający się nieco ponad milę od centrum miasta do portu promowego jest niczym oświetlony neonami plac zabaw dla dzieci. Kobiety i osoby o bardziej skomplikowanej definicji płciowej oblegają ulice, zachęcając klientów do korzystania z ich usług towarzyskich.



Cudzoziemscy asystenci policji FTPA

Innym ciekawym pomysłem, choć dla Europejczyka zaskakującym, jest instytucja „skrzynki policyjnych” instalowanych na obrzeżach przedsięwzięć biznesowych. Cudzoziemiec zakładający firmę w Tajlandii otrzymuje od policji propozycję kupienia tzw. skrzynki policyjnej. Prosta skrzynka odpowiednio oznaczona zawiera coś, co w Europie nazwalibyśmy „książką przebiegu służby”. Dzielnicy ma obowiązek systematycznego sporządzania krótkich notatek z zakresu bezpieczeństwa w formie raportu z obchodu w okolicy ustawienia skrzynki. Takie wizyty w firmie odbywają się codziennie pomiędzy godz. 16.00 a 17.00. Policjant pyta personel o ewentualne problemy, odnotowuje wszelkie

STRUKTURA ORGANIZACYJNA BMA



ETAPY STRATEGII ODPORNOŚCI BANGKOKU



uwagi. Płacąc niewielki abonament, właściciel biznesu ma zapewniony serwis policji, a w przypadkach kwestii spornych jest traktowany z większą życzliwością.

Struktura strategii odporności Bangkoku

Strategię w imieniu władz miasta zamówił organ o nazwie Bangkok Metropolitan Administration (BMA). Jej opracowanie rozpoczęło od warsztatów ustalania agendy we wrześniu 2014 r. (dokument upubliczniono w lutym 2017 r.). Następnie podjęto badania i konsultacje, aby lepiej poznać wyzwania stojące przed miastem. Seria dużych warsztatów z udziałem sektorów publicznego i prywatnego, społeczeństwa obywatelskiego, środowisk akademickich i mieszkańców Bangkoku ujawniła różnice w postrzeganiu wyzwań związanych z odpornością miasta, zarówno w codziennych warunkach, jak i w okresach zwiększonego stresu, np. bezpośrednio po powodziach w 2011 r. W konsultacjach wzięło udział ponad 500 osób. Odpowiadali na pytania związane z 12 czynnikami zwiększającymi odporność, które obejmują City Resilience Framework (CRF). CRF pozwoliło uczestnikom na kompleksową identyfikację mocnych i słabych stron miasta. Opracowano wstępną ocenę odporności, która podsumowała ustalenia z tego procesu i zaproponowała kluczowe obszary do dalszego badania.

Strategie miast mają różną strukturę, stawiają różne cele oraz daty wypełnienia postulatów. Za każdym z zadań stoją opisane zadania szczegółowe oraz narzędzia i technologie wspierające procesy. Wszystko zależy od realnych potrzeb i uwarunkowań miasta. Programy szczegółowe strategii mają każdorazowo taką samą strukturę z podziałem na wskazanie:

- które agencje i wydziały są odpowiedzialne za wykonanie zadania oraz podanie ich partnerów,
- jak jest oceniana ważność czynnika odporności,
- kto jest beneficjentem zrealizowania zadania,
- krótki opis realizacji zadania,
- ramy czasowe przewidziane na wykonanie zadania.

Cele strategiczne powołują się na doświadczenia miast o podobnych problemach (najczęściej z sieci współpracy organizacji 100 Resilient Cities). Przykładowo w sprawach dotyczących transportu publicznego punktem odniesienia dla Bangkoku było Mexico City, a dla celu zarządzania zasobami wodnymi – Rotterdam. W obszarze wymiany doświadczeń w zakresie radzenia sobie ze skutkami powodzi i przypływów Bangkok czerpał z doświadczenia Nowego Orleanu i Mexico City.

Oprócz powodzi Bangkok jest narażony na wstrząsy i stesy dotyczące mieszkańców, z których wiele prawdopodobnie ulegnie zaostrzeniu w wyniku zmian klimatu. Ważne, aby społeczność miejska posiadała wiedzę i umiejętności umożliwiające radzenie sobie z nimi. Zostanie ona włączona we wszystkie inicjatywy administracyjne BMA dotyczące odporności miast. Skuteczne systemy komunikacji za pośrednictwem wielu kanałów i sieci poprawiają szybkość monitorowania sytuacji awaryjnych oraz czujność i szybkość reakcji. Administracja miasta, wraz z zagrożonymi społecznościami, postawiła sobie za cel wdrożenie większego wykorzystania technologii łączności stosowanych w życiu codziennym przez mieszkańców do celów komunikacji kryzysowej w przypadku zagrożeń naturalnych lub innych katastrof i kryzysów.

W obszarze rozwiązań komunikacji punktem odniesienia dla Bangkoku było miasto Berkeley, które pracuje nad



budowaniem przygotowanej na czas kryzysu „cyfrowej” społeczności. Uruchamia program Community Resilience Centre (CRC), pomocny w reagowaniu na zachodzące katastrofy. Berkeley wspiera również łączność sąsiedzką na wypadek katastrof poprzez partnerstwo z liderami społeczności lokalnych i organizacjami pozarządowymi (łączniki gotowości na wypadek katastrofy sąsiedzkiej).

Jednym z zadań szczegółowych wymienionych w strategii *urban resilience* jest powołanie centrum edukacji postkryzysowej. Pierwsze takie centrum w Bangkoku zostało zaprojektowane i zbudowane w Departamencie Pożarnictwa i Ratownictwa BMA, aby zapewnić możliwość studiowania przypadków i okoliczności im towarzyszących po trzęsieniach ziemi i pożarach. Celem centrum jest nawiązywanie kontaktów ze społeczeństwem na temat zagrożeń i możliwych skutków katastrof, sposobów reagowania i przetrwania w nieoczekiwanych okolicznościach oraz wskazówek dotyczących bezpieczeństwa. Centrum demonstruje także zdolność BMA do zarządzania klęskami żywiołowymi w celu budowania zaufania i poczucia bezpieczeństwa mieszkańców i turystów.

Innym zadaniem jest głębsze wykorzystanie aplikacji na smartfony w modelu *blockchain*. W tym projekcie testuje się wiele aplikacji na urządzenia mobilne w zakresie gotowości na wypadek powodzi i katastrof. Bangkok dysponuje znaczną ilością da-

nych pomocnych w przewidywaniu klęsk żywiołowych i projektowaniu postępowania w sytuacjach kryzysowych. Nie wszystkie informacje jednak są łatwe do zlokalizowania, zrozumienia lub wykorzystania operacyjnego. Aby wspierać zarządzanie kryzysowe, baza danych GIS w Bangkoku, opracowana przez straż pożarną i ratowniczą, będzie musiała zostać rozszerzona w zakresie różnorodności istotnych danych, objętości, dokładności, niezawodności i sieci z innymi źródłami danych, również innych prowincji.

Baza danych i baza danych o katastrofach w Bangkoku zostanie opracowana jako kompleksowe centrum online dla różnych rodzajów informacji na temat katastrof i zagrożeń. Będzie także działać jako repozytorium siły roboczej, umiejętności, maszyn i pojazdów do mobilizacji zasobów w operacjach awaryjnych oraz jako analiza skutków oparta na scenariuszach za pośrednictwem sieci udostępniania i przesyłania danych. Ma również generować mapy 3D na podstawie danych geoprzestrzennych i danych podstawowych, wspierając zespoły ratownicze BMA.

Miasto Bangkok, przy pomocy organizacji 100 RC, opracowało strategię, zgodnie z którą zobowiązało się do realizacji 18 inicjatyw obejmujących 57 projektów określonych w niej. Okres ich realizacji ze względu na bardzo ambitne założenia został rozłożony na rok do 5 lat. Naturą projektów i metodologii *resilience* jest dzia-

łanie w interdyscyplinarnych zespołach zadaniowych. W przypadku Bangkoku są to zespoły:

- powodzi,
- mobilności,
- gospodarki i równości społecznej,
- ds. ochrony zdrowia i dobrostanu,
- ds. zmniejszania wpływu kryzysów i wstrząsów oraz „szoków” życia miejskiego; w tym zespole umieszczono sferę metropolitalnego zarządzania kryzysowego,
- zbiorowy, integrujący działania różnych organizacji zaangażowanych w rozwój strategii; pracują w nim przedstawiciele policji metropolitalnej.

Analizując skład tych zespołów oraz umiejscowienie struktur policji, można odnieść wrażenie, że bezpieczeństwo miasta – rozumiane jako prewencja kryminalna czy działania antyterrorystyczne – są daleko w tle lub wręcz niewidoczne. W Bangkoku, jeszcze przed procesem tworzenia strategii *resilience*, przeprowadzono szczegółowe badanie przydatności wraz z rekomendacjami rozwoju dla systemu CCTV funkcjonującego w mieście. Analiza ta stanowiła solidny grunt działań nad strategią. Tak jest tylko pozornie, gdyż celem zapewnienia odporności jest wysoki standard życia mieszkańców. Ten wymóg zawsze jest powiązany z bezpieczeństwem osobistym czy biznesu. Niemniej należy postrzegać ten trend jako wyzwanie niedalekiej przyszłości.

Zabezpieczenia techniczne w Bangkoku

Od roku 2011 BMA wraz z ministerstwem spraw wewnętrznych podejmują działania w kierunku rozbudowy systemu monitoringu wizyjnego w Bangkoku. Były one elementem szerszego projektu odnowienia infrastruktury CCTV w całej Tajlandii, który zakładał zainstalowanie 360 tys. kamer. Warto dodać, że jednym z pierwszych wróżen, jakie odnosi się, spacerując po mieście, jest wszechobecność kamer monitoringu zainstalowanych przez prywatne firmy na prywatnych budynkach. Obejmują one zasięgiem nie tylko obszar firmy, ale także dużą przestrzeń publiczną. Policja w razie konieczności szeroko korzysta z zapisów z tych kamer, co z reguły nie budzi sprzeciwu właścicieli firm i sprzętu.



Niska jakość obrazów z kamer monitoringu miejskiego (z zamachu w 2015 r.) uniemożliwiła zidentyfikowanie sprawcy

Dla skutecznego przeprowadzenia inwestycji w system kamer stanowiących własność rządu przeprowadzono badanie potrzeb w zakresie poziomu bezpieczeństwa w mieście i uzasadnienia ich zainstalowania. To badanie ilościowe miało na celu określenie związku między zaufaniem społeczeństwa do zastosowania monitoringu wizyjnego w polityce kontroli przestępczości w Bangkoku a strachem przed przestępczością wśród mieszkańców. Wynikiem badania była konstatacja o niewystarczającej liczbie kamer, przy jednoczesnym niewłaściwym wykorzystaniu już działających. Konieczne więc było wypracowanie rozwiązania kompromisowego.

W styczniu 2015 r. gubernator potwierdził, że BMA ma już 50 tys. kamer obejmujących zasięgiem wszystkie obszary Bangkoku, chociaż jest to liczba mała w porównaniu z całkowitą powierzchnią Bangkoku (1569 km²) – jedna kamera przypada na 31 380 m², co nie wystarczy, aby powstrzymać przestępczość. W Londynie o porównywalnej powierzchni (1572 km²) jest 8 razy więcej kamer niż w Bangkoku. Mieszkańcy Bangkoku nie byli jednocześnie przekonani co do skuteczności kamer. Badanie wykazało, że nie wierzą, iż wszystkie instalacje CCTV zainstalowane przez BMA są sprawne. Społeczeństwo uważa też, że liczba kamer zainstalowanych przez BMA jest niewystarczająca. Co interesujące, mieszkańcy w badaniu nie dowierzali też, że BMA ma wystarczającą liczbę pracowników (operatorów), aby monitorować zachowania przestępców za pośrednictwem telewizji dozorowej. Zaskakuje bardzo dojrzała uwaga wyrażona w opinii publicznej, podająca w wątpliwość wysokiej klasy koordynację pomiędzy policją metropolitalną a BMA, czyli administracją miasta. Jeśli chodzi o publiczny lęk przed przestępczością, badanie wykazało, że był on na umiarkowanym poziomie.

W efekcie wypracowano rekomendacje o zwiększeniu liczby kamer z 50 do 60 tysięcy. Jednocześnie zobligowano BMA

do ustanowienia specjalnego działu odpowiedzialnego za konserwację i naprawę zainstalowanych systemów monitoringu. Ta sugestia wynika z ustalenia, że brak pewności co do lokalizacji kamer i jakości obrazu powoduje większy niepokój przed przestępstwem. Przypomniano sytuację z zamachu bombowego w Tajlandii w 2015 r. na świątynię Erawan w Bangkoku, w którym zginęło 20 osób, a ponad 100 zostało rannych. Niestety doszło wtedy do blamażu zarówno policji, jak i miejskiego systemu monitoringu wizyjnego. Udało się odtworzyć postać zamachowca, ale bez możliwości rozpoznania szczegółów. Zawiódł źle funkcjonujący system CCTV. Sprawca, uciekając, był teoretycznie w zasięgu 20 kamer, ale tylko pięć działało. Piętnaście było uszkodzonych. Sprawcy nie wykryto do dzisiaj.

W Bangkoku rezyliencja „pachnie” bardziej dbałością o rozwój miasta niż bezpieczeństwem

Krótki opis założeń strategii odporności miasta to jedynie zarysowanie treści ze 128 stron raportu strategii, którą Bangkok Metropolitan Administration przygotowało wspólnie z organizacją 100 Resilient Cities w 2017 r. Dokument jest pełen wytycznych zarówno organizacyjnych, jak i technicznych. Jako taki stanowi dobrą podstawę do rozpoczęcia planowania procesu inwestycyjnego również w bezpieczeństwo miasta. Przykładem są np. kwestia inwestycji w miejski system CCTV oraz wytyczne dotyczące poprawy monitorowania i konserwacji systemów. Szeroka dostępność aplikacji na urządzenia mobilne obywateli czy systemy komunikacji w sytuacjach kryzysowych dają duże możliwości osobom tradycyjnie zajmującym się bezpieczeństwem w organizacjach oraz bezpieczeństwem publicznym.

Sytuacja ta stanowi wyzwanie dla profesjonalistów branży bezpieczeństwa publicznego i organizacji. Zarówno tych, którzy zakończyli już karierę w służbach mundurowych, jak i zdobywających swoje profesjonalne szlify ochrony w biznesie.

Analiza strategii wprowadzonej w Bangkoku pokazuje, że wszędzie tam, gdzie władze miejskie zaczynają myśleć o zarządzaniu miastem w kontekście odporności, a w obszarach bezpieczeństwa i zarządzania kryzysowego tam, gdzie jest to prawnie możliwe, metody *resilience* wchłaniają tradycyjne funkcje bezpieczeństwa.

Sytuacja ta stanowi wyzwanie oraz szansę na rozwój dla dzisiejszych security managerów, którzy są niejako naturalnymi kandydatami na objęcie stanowisk resilience managerów zarówno organizacji, jak i miast. Do tego należy się bardzo gruntownie przygotować. ▣

B I O

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. Entuzjasta bezpieczeństwa miast, realizujący swoją pasję w powstającej pracy doktorskiej.



Głos. branży

JAK BRANŻA SECURITY MOŻE POMÓC W ZAPEWNIENIU BEZPIECZEŃSTWA MIESZKAŃCOM MIAST W DOBIE PANDEMII? GŁOS ZABIERAJĄ PRZEDSTAWICIELE RÓŻNYCH SEKTORÓW GOSPODARKI.



Leszek Lawera

IBM

Informatyczne aspekty bezpieczeństwa

Od lat jestem związany z branżą informatyczną, więc skupię się tylko na informatycznych aspektach bezpieczeństwa.

Na pierwszy plan wysuwają się zagadnienia związane z przetwarzaniem obrazu, termowizją, monitorowaniem kontaktów fizycznych pomiędzy ludźmi w przestrzeni publicznej, transporcie itp. oraz cyberbezpieczeństwem i użyciem analizy (zaawansowanych technologii AI oraz *big data*) szeroko rozumianych social mediów w celu diagnozy stanu populacji miast, regionów czy województw.

1. Przetwarzanie obrazu wideo oraz termowizja

Z punktu widzenia branży security najważniejsze wydaje się monitorowanie bezpiec-

nej odległości pomiędzy ludźmi w obszarach objętych ochroną. Obecne na rynku systemy umożliwiają alertowanie wielu sytuacji, takich jak:

- zwiększona liczba osób na danym terenie,
- naruszanie stref bezpieczeństwa,
- nieprzestrzeganie regulaminowych odległości (np. w kolejce do kasy).

Konfiguracja takiego systemu nie była rzeczą prostą, a technologiczne możliwości kamer, ich własne możliwości analityki obrazu oraz analityka *streamingu* z kamery zwykle nie były implementowane ze względu na koszt i pracochłonność wdrożenia. Wobec spadku cen urządzeń, wzrostu wydajności procesorów przetwarzania obrazu oraz widocznego nacisku biznesowo-społecznego na funkcjonalność takich rozwiązań sytuacja może się zmienić. W najbliższej przyszłości może nas czekać boom dotyczący rozbudowy systemów monitoringu wizyjnego z zaawansowanymi technologiami analizy strumienia wideo – AI (sztucznej inteligencji) oraz *deep learningu*.

Nieco inaczej ma się rzecz z termowizją. Obserwujemy gwałtowny skok technologiczny urządzeń związanych z pomiarem temperatury. Systemy kamer termowizyjnych bardzo szybko się rozpowszechniają, monitorując wejścia do obiektów i przestrzenie publiczne typu dworce i lotniska – nie jest to jednak panaceum na rozprzestrzenianie się wirusa. Poza technicznymi możliwościami istotnymi czynnikami zniechęcającymi potencjalnych zainteresowanych jest wysoka skuteczność powszechnie dostępnych leków przeciwgorączkowych oraz fakt, iż część zainfekowanych przechodzi chorobę bezobjawowo.

2. Aplikacje mobilne

Obecnie nie ma już chyba obszaru naszego życia, w którym nie można zastosować aplikacji mobilnej, w tym również monitorowania przebiegu kwarantanny i szybkiego diagnozowania osób potencjalnie narażonych na kontakt z chorą osobą. W Singapurze władze wprowadziły aplikację Trace Together, która informowała jej właściciela, że w zasięgu Bluetooth znalazł się potencjalny nosiciel wirusa. W Hongkongu władze egzekwują noszenie specjalnej bransoletki połączonej ze smartfonem, która informuje odpowiednie służby, że dana osoba opuszcza miejsce kwarantanny. W Korei Południowej rząd użył informacji z kart kredytowych, danych lokacyjnych ze smartfonów i rozbudowanego monitoringu wizyjnego do tworzenia map, gdzie możemy być narażeni na kontakt z wirusem. Dotychczas wprowadzone rozwiązania nie uwzględniały kwestii bezpieczeństwa danych

i prywatności obywateli. Wobec groźby pandemii rządy i służby państwowe usankcjonowały prawnie niektóre rozwiązania znacznie ograniczające prywatność i bezpieczeństwo danych osób poddanych kwarantannie. Rządowa agencja bezpieczeństwa w Izraelu wprowadziła aplikację kontrolującą osoby poddane kwarantannie bazującą na lokalizacji smartfona danej osoby. Okazało się jednocześnie, że agencja zbiera te dane już od ponad dwóch lat pod pretekstem walki z terroryzmem.

Żeby nie być do końca pesymistą w sprawie ochrony danych osobowych – a w konsekwencji naszej wolności obywatelskiej – podam pozytywny przykład aplikacji napisanej w Massachusetts Institute of Technology (MIT) – nazwanej Private Kit: Safe Paths. Idea – niestety dosyć utopijna – zakłada, że każdy sam będzie odpowiedzialny za aktualność informacji o stanie swojego zdrowia, a informacje wrażliwe zostaną zaszyfrowane i pozostaną w urządzeniu użytkownika. Urządzenia będą komunikować się między sobą bez użycia danych wrażliwych, a zainteresowani otrzymają jedynie informację, czy w pobliżu znajduje się ktoś z koronawirusem, czy nie. Słabością rozwiązania jest bezpośredni związek skuteczności działania z powszechnością jego zastosowania.

3. Cyberbezpieczeństwo

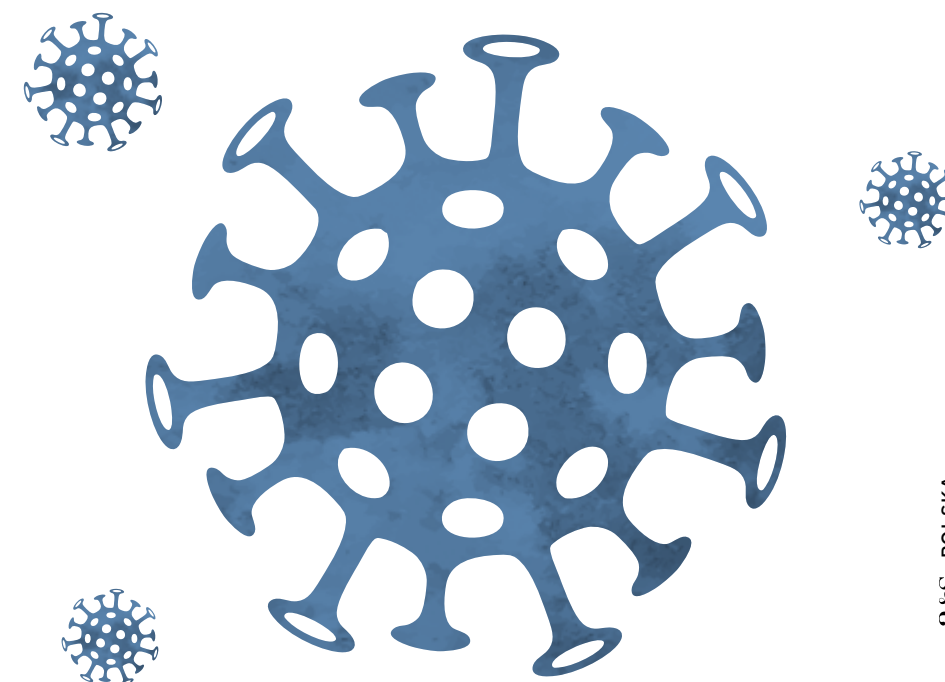
Zwiększona aktywność w sieci Wi-Fi osób prywatnych, które przeniosły miejsce pracy do domu, jest potencjalnym obszarem ataku i realnym zagrożeniem. Nie wszystkie organizacje są na to przygotowane od strony zarówno technologicznej, jak i organiza-

cyjnej. Szczególnie niskie w tym przypadku okazały się świadomość i wiedza użytkowników. Otwiera to nowe rynki i możliwości dla firm, produktów i przede wszystkim szkoleń, ponieważ od tego momentu praca z domu stanie się zjawiskiem trwałym i powszechnym.

4. Analiza mediów społecznościowych

W ostatnich latach mechanizmy *big data* oraz zastosowanie sztucznej inteligencji do analizy tekstu w szeroko pojętych mediach społecznościowych pozwoliły na wyciąganie bardzo dokładnych wniosków dotyczących kondycji całych grup społecznych czy trendów społecznych (w tym niestety preferencji wyborczych), co można wykorzystać do diagnozy stanu zdrowotnego konkretnej grupy czy populacji. Analiza zapytań w popularnych przeglądarkach o konkretny objaw fizjologiczny jest ściśle skorelowana z wystąpieniem tych objawów na danym terenie czy obszarze. Odpowiednie wykorzystanie tych informacji może pomóc w decyzjach administracyjnych związanych z pandemią.

Jak widać, akcentem, który ciągle się przewija w każdym zagadnieniu związanym z bezpieczeństwem, jest utrzymanie stanu równowagi pomiędzy skutecznością działania a zachowaniem praw obywatelskich, prywatności i wolności jednostki. Kryzys pandemii uświadomił wszystkim, że zachowanie tego stanu równowagi w sytuacjach kryzysu, strachu i niepewności jest niezwykle ważne – a po przekroczeniu pewnej granicy władza administracyjna (jakakolwiek by ona była) nie zechce oddać dobrowolnie tak uzyskanej kontroli. ↗





Konrad Badowski

Axis Communications

Najnowsza technologia szansą na oszczędności

Do tej pory wizyty u lekarza, spotkania biznesowe, zajęcia na uczelniach czy zebrania firmowe odbywały się najczęściej fizycznie, w świecie realnym. Często traciliśmy czas na dojazdy czy oczekiwanie w kolejkach. Od kilku tygodni znaczna część naszego zawodowego i prywatnego życia przeniosła się do sieci i, wbrew obawom, całkiem dobrze przechodzimy ten przyspieszony kurs digitalizacji. Pandemia koronawirusa sprawiła, że wstrzymane wcześniej plany cyfrowych wdrożeń w wielu firmach musiały zostać zrealizowane. Jeszcze kilka tygodni temu nie mieliśmy tak dużych potrzeb, szczególnie tych związanych z pracą zdalną. Dziś one się pojawiły, co zdecydowanie przyspieszyło realizację projektów digitalizacji. Może się nawet okazać, że po ustaniu pandemii wielu pracowników pozostanie w domach. Szacuje się, że na stałe zdalnie może pracować do 30% z nich.

Sytuacja, z jaką obecnie mamy do czynienia, może być dla firm wielką szansą na znalezienie nowych oszczędności. Koszty utrzymania biur są dzisiaj znaczne, a to, co dzieje się aktualnie, pozwala rozprawić się z wieloma mitami dotyczącymi pracy zdalnej. Ten czas spędzony poza biurem już pokazuje, że da się tak pracować i że jest to praca bardzo efektywna.

Jednym z przykładów dziedziny, która na pandemii może zyskać, jest niewątpliwie medycyna, a dokładnie telemedycyna. Technologia zwiększa dostępność do niektórych usług medycznych, ale także pozwala na monitorowanie stanu pacjenta bez

konieczności narażania personelu medycznego na zakażenie. Nowoczesne kamery IP zintegrowane z systemem audio i kontrolą dostępu znacznie minimalizują takie ryzyko, a trzeba pamiętać, że problem zakażeń podczas pobytu w szpitalu był bardzo poważny jeszcze przed pandemią.

Coraz częściej kamery i interkomy IP są integrowane z łóżkami przeznaczonym dla oddziałów IOM i dostarczane szpitalom jako kompletne rozwiązanie, dzięki któremu personel medyczny jest w stanie obserwować i komunikować się z pacjentem w sposób bezpieczny i efektywny.

Ogromną szansą na dalsze zwiększenie funkcjonalności takich rozwiązań jest możliwość integracji kamer z czujnikami medycznymi poprzez otwarte API lub dedykowane oprogramowanie analityczne. Kamery obserwujące pacjentów mogą także automatycznie wykrywać np. upadek z łóżka. Zazwyczaj czas reakcji na takie zdarzenie jest kluczowy dla zdrowia pacjenta. Jak pokazują zrealizowane projekty, często nie trzeba wymyślać nowych rozwiązań, w szpitalach z powodzeniem sprawdzają się systemy oryginalnie projektowane dla handlu lub infrastruktury krytycznej. Te pierwsze pomagają lepiej dopasować przestrzeń szpitalną do poruszających się po niej lekarzy, pacjentów i odwiedzających, a drugie z powodzeniem chronią sprzęt medyczny i leki przed niepożądanym dostępem. Pandemia COVID-19 raczej nie zmienia kierunku, w którym podąża telemedycyna, natomiast na pewno przyspieszy ten proces. Myślę, że w tym aspekcie możemy szukać pozytywów sytuacji, w jakiej się znaleźliśmy.



Przemysław Bańko

Omniconnect

Nowoczesne technologie w walce z kryzysami

Mówiąc o bezpieczeństwie mieszkańców w kontekście pandemii, musimy przede wszystkim myśleć o ich zdrowiu, wymuszaniu prawidłowych zachowań i respektowaniu przez mieszkańców wytycznych minimalizujących rozszerzenie się pandemii. Branża security oferuje wiele skutecznych systemów wspierających decyzje i zarządzanie miastem. Systemy monitoringu wizyjnego umożliwiające nadzór nad poszczególnymi strefami miasta. Elektroniczne tablice informacyjne, które mogą służyć do komunikacji z mieszkańcami i informowania o pandemii oraz środkach zabezpieczania. Systemy powiadamiania SMS-em – niezwykle ważne w komunikacji w trakcie kryzysu epidemicznego. Automatyczne kurtyny odkażające mogące mieć doskonałe zastosowanie w bezpiecznej logistyce mieszkańców. Systemy pracy zdalnej umożliwiające naukę w czasie pandemii. Systemy handlu elektronicznego i płatności redukujące w założeniu liczbę osób poruszających się po miastach. Liczniki przejść, które w istotny sposób automatyzują zliczanie klientów w środkach komunikacji czy sklepach. Można wymieniać dziesiątki innych systemów. Pozostaje tylko pytanie, czy te i inne systemy zostały w trakcie obecnej pandemii skutecznie wykorzystane. W mojej ocenie – NIE. Postrzegając pandemię jako ogromny globalny kryzys zdrowotny, gospodarczy i społeczny, powinno się natychmiast uruchomić grupy eksperckie, aby wypracowały standardy bezpiecznego wykorzystania zdobytych naukowych i technologicznych w walce

z epidemią. Pamiętajmy bowiem, że takie pandemie jak obecna staną się codziennością. Z badań publikowanych przez WHO można wywnioskować, iż będziemy mieli z nimi do czynienia co 3–4 lata. Ważne, abyśmy potrafili dzisiejsze niepowodzenia przekuć w szansę na przyszłość. Obecny trudny czas, chaotyczne decyzje lub ich brak, problemy z wykorzystaniem elektronicznych systemów zabezpieczania i wspierania zarządzania miastem musimy po prostu przeżyć. ŻŁE JEDNAK BĘDZIE, JEŚLI dzisiejsze: niefrasobliwość i amatorszczyzna, brak procedur i planów kryzysowych, a jeśli już były – brak ich testowania, brak szybkich i zdecydowanych rozwiązań STANĄ SIĘ NASZYM STANDARDZEM.

Nauczmy się lepiej wykorzystywać nowoczesne, bezpieczne technologie do walki z kolejnymi kryzysami. Tak naprawdę w zakresie know-how jesteśmy w XXI wieku, ale umiejętności korzystania z nich pozostawiają niestety wiele do życzenia.



Rafał Batkowski

RBStrategie

Asystent bezpieczeństwa wesprze mieszkańców

Pandemia SARS-CoV-2 zmienia tradycyjne myślenie o bezpieczeństwie i zmusza samorządy miast do zwrócenia większej uwagi na poczucie bezpieczeństwa mieszkańców. Sytuacja pozwala przewidywać rosnącą rolę podmiotów prywatnych dostarczających usługi ochrony i technologie bezpieczeństwa.

„Poczucie bezpieczeństwa” nie jest tożsame z realnym stanem zagrożeń. Niedocenywanie rzetelnej, opartej na faktach komu-



nikacji z mieszkańcami, braki w zakresie edukacji społecznej służącej zapobieganiu zagrożeniom i budowaniu właściwych postaw w obliczu niebezpieczeństwa może znacząco zaburzać postrzeganie środowiska bezpieczeństwa. Strach, obawa przed zarażeniem, brak zaufania do instytucji medycznych, stosowanych procedur sanitarnych może destabilizować relacje grupowe, rówieśnicze, pracownicze i rodzinne, a izolacja wprost wpływać na stan psychofizyczny ludzi. Przeciwdziałanie tak określonym zagrożeniom związanym z epidemią jest zadaniem państwa i samorządu. Miasta i ich władze, aktywizując obszary współpracy w sferze cyfrowej z mieszkańcami, wzmacniając przekaz dotyczący stanu zagrożeń, dobrze sobie radzą z sytuacją odczuwania bezpieczeństwa w środowisku lokalnym.

Spojrzenie sprzed pandemii, odwołujące się głównie do kompetencji służb państwowych i straży miejskich, nie jest dzisiaj wystarczające. Strategie rozwoju miast rzadko uwzględniały aspekty kontroli przestępczości i redukcji zagrożeń kryminalnych, stąd potrzeba szukania nowych rozwiązań, w tym czerpania z kompetencji firm prywatnych dostarczających technologie bezpieczeństwa, a także fizyczną ochronę obiektów i obszarów. Nie chodzi jedynie o dyskusję na temat implementacji kontrolerów dostępu z zaawansowaną detekcją twarzy i pomiarem temperatury, ale o znacznie szerszy obszar rozważań, m.in. zabezpieczenie przed nieautoryzowanym dostępem do szpitali miejskich i placówek leczniczych dedykowanych walce z COVID-19; ochrona urzędów miast i innych obiektów miejskich niepodlegających obowiązkowej ochronie; identyfikacja potencjalnie chorych; wprowadzanie procedur

sanitarnych i szkolenia miejskich urzędników; monitorowanie sytuacji w fazie „odmrażania” itd.

Zagadnieniem wielkiej wagi jest utrzymanie ciągłości działania instytucji miejskich, z uwzględnieniem formy kontaktów „na odległość”. Każdy zarządzający miastem w kryzysie powinien brać pod uwagę znaczący potencjał nowych technologii i profesjonalizm wielu formacji ochronnych oraz inne inicjatywy, takie jak Asystent Bezpieczeństwa firmy RBStrategie, który ma służyć niezależnemu wsparciu mieszkańców w sprawach dotyczących ich bezpieczeństwa.



Marcin Walczuk

BCS

Bezpieczne zmiany w czasie pandemii

Na świecie pozostaje niewiele branż, których nie dotknął wybuch pandemii koronawirusa. Praktycznie w każdym sektorze gospodarki notuje się większe lub mniejsze straty. Podobnie rzecz się ma w branży security, w której menedżerowie też muszą szukać nowych rynków zbytu dla swoich produktów, aby uniknąć konieczności redukcji etatów. Na szczęście z pomocą przychodzą im działy rozwoju produktów, proponując nowe rozwiązania specjalnie skrojone pod kątem sytuacji, w której się znaleźliśmy. Oczywiście miejsc, gdzie te produkty będzie można wykorzystać, jest wiele. Nowe możliwości zastosowań chciałbym przybliżyć na przykładzie mi najbliższym, czyli jak zmieniło się biuro BCS od momentu rozpoczęcia pandemii i jak wygląda teraz, kiedy wszyscy powoli wracamy do pracy. Wprowadzeniu każdej zmiany przyświecał oczywiście nadrzędny cel,



jakim jest zapewnienie bezpieczeństwa pracownikom, ale trzeba było to pogodzić z normalnym w miarę funkcjonowaniem firmy.

Z istotnych zmian, jakie zostały wprowadzone, było pojawienie się przy wejściach do firmy kamer termowizyjnych. Ich zadaniem jest wykonanie automatycznie pomiaru temperatury każdej wchodzącej do budynku osoby. Dane z pomiaru są przetwarzane przez rejestrator wchodzący w skład systemu do pomiaru temperatury ciała człowieka, w przypadku zbyt wysokiej natychmiast uruchamiany jest alarm. Wartość temperatury, przy której taki alarm będzie się uruchamiał, można dowolnie określić. Jeśli ustalony próg zostanie przekroczony, pomiar jest powtarzany przy użyciu ręcznego termometru bezdotykowego.

Ze względu na konieczność zachowania dystansu społecznego w miejscach, gdzie do tej pory ludzie gromadzili się najliczniej, został zastosowany system liczenia osób, w którym można określić liczbę osób mogących wejść do danego pomieszczenia. Jest to realizowane za pośrednictwem kamery BCS Line z serii AI, która kontroluje wejście do strefy i w razie uzyskania limitu osób uruchamia alarm trwający, dopóki liczba ta nie zmaleje. Gdy do danej strefy jest kilka wejść czy wyjść, kilka takich kamer można ze sobą połączyć za pośrednictwem rejestratora serii NVR-4K-III, który może kontrolować do 4 przejść równocześnie, prowadząc wspólną statystykę.

Kolejnym ograniczeniem, jakie wprowadziliśmy, było odseparowanie od siebie poszczególnych działów firmy. Drzwi między nimi zostały zamknięte, a kontrolę nad nimi sprawuje teraz bezdotykowy system kontroli dostępu współpracujący z kamerą z funkcją identyfikacji twarzy. Kontroler z taką kamerą identyfikuje osobę na podstawie zapisanej bazy danych twarzy. Jeśli porównanie będzie prawidłowe, zostanie przyznany dostęp do kolejnej strefy. Jako dodatkową funkcję ochronno-kontrolną można wykorzystać wykrywanie maseczki ochronnej na twarzy osoby znajdującej się przed kamerą.

Przytoczone przykłady są tylko częścią wprowadzonych przez nas zmian, ale te wykorzystują rozwiązania techniczne, które my, jako BCS, możemy zaproponować innym, by również mogli poczuć się bezpiecznie. Czy będzie to mała firma, placówka służby zdrowia, czy sklep wielkopowierzchniowy, wszędzie tam, stosując któryś ze wspomnianych systemów, można wydatnie podnieść poziom bezpieczeństwa, bo przecież chodzi o to, żebyśmy byli zdrowi i bezpieczni.



Piotr Bettin

Konica Minolta

Systemy zabezpieczeń w nowoczesnym mieście

Systemy zabezpieczeń powinny przede wszystkim wspierać zarządzanie miastem i umożliwiać wgląd w to, co dzieje się w przestrzeni publicznej – monitorować zachowania ludzi, wskazywać miejsca, gdzie się gromadzą itp. Kluczowe jest jak najszybsze otrzymanie przez operatora sygnału o sytuacjach niebezpiecznych. Na rynku dostępne są rozwiązania monitoringu wizyjnego wyposażone w algorytmy wykrywające podejrzane zachowania – bójki, zaśląbnięcia, zamieszki czy potencjalne stany paniki, np. biegnących ludzi. W każdej z tych sytuacji system automatycznie przetwarza obrazy w czasie rzeczywistym i wysyła alarmy do odpowiednich służb. Algorytmy sterowane sztuczną inteligencją analizują dane o wiele szybciej niż człowiek, co zwiększa skuteczność reakcji i redukuje liczbę fałszywych alarmów nawet o 90%. Popularność zyskują również systemy analizy dźwięku, które umożliwiają

kategoryzowanie dźwięków (strzały, wybuchy, syreny, krzyk). Czas ich wykrycia i klasyfikacji to zaledwie milisekundy.

Przy wyborze rozwiązań monitoringu wizyjnego miasto powinno przede wszystkim zwracać uwagę na to, czy są one kompatybilne z pozostałymi funkcjonującymi już systemami. Tego typu inwestycje są z reguły długoterminowe, technika i technologia powinny więc umożliwiać rozwiązywanie nie tylko dzisiejszych problemów, ale także tych, które dopiero się pojawią za 5 czy 10 lat. Oczywiście nie sposób przewidzieć, przed jakimi wyzwaniami staną wtedy miasta, dlatego platformy powinny być otwarte i umożliwiać dodawanie nowych funkcjonalności w miarę pojawiających się potrzeb, np. gdy będzie niezbędne monitorowanie przepływu ludzi na ścieżkach rowerowych i na tej podstawie zaplanowanie kolejnych inwestycji w infrastrukturę.

System, który nie współdziała z innymi rozwiązaniami i urządzeniami, ogranicza inwestora i może uzależnić miasto od jednego producenta, a ten może nie mieć w ofercie wszystkich potrzebnych w przyszłości funkcji. W efekcie ogromne kwoty zostaną wydane na platformę, która nie zapewni potrzebnych funkcjonalności i uniemożliwi ich zakup u innego dostawcy. System powinien więc być niezależny od producentów. Ważna jest dostępność API (*interfejs programowania aplikacji, application programming interface*) oraz SDK (*software development kit, narzędzia do tworzenia aplikacji*), które umożliwią samodzielne rozbudowywanie platform i oprogramowania, np. przez zewnętrznego programistę, gdy pojawi się taka potrzeba. Jeszcze pół roku temu nikt nie spodziewał się, że potrzebne będzie oprogramowanie do wykrywania ludzi bez maseczek, algorytmy analizujące odległości między ludźmi na ulicy i wykrywające skupiska ludzi czy mierzenie temperatury osobom wchodzącym do urzędu. Sytuacja i warunki, w jakich działają miasta, ciągle ewoluują, potrzebna jest więc otwarta technologia, umożliwiająca nadążanie za zmianami i reagowanie nawet na to, czego nie jesteśmy w stanie przewidzieć.



Robert Sienkiewicz

Dahua Technology Poland

Miejski system monitoringu wizyjnego w dobie epidemii

Dotychczas włodarze miast skupiali się na zapewnianiu bezpieczeństwa i ułatwianiu mieszkańcom funkcjonowania, aż do chwili, gdy przyszło się zmierzyć z nieoczekiwanym wrogiem – COVID-19. W tej sytuacji należało zastosować nową strategię. Narzędziami wspierającymi w walce z epidemią mogą być nowoczesne systemy wizyjne, platformy i technologie inteligentnych miast. Trzeba też pamiętać, że nie jesteśmy przygotowani na nowe zdarzenia, takie jak ekstremalne zjawiska atmosferyczne związane ze zmianą klimatu.

Chciałbym skupić się na trzech wybranych technologiach, które moim zdaniem znalazły zastosowanie w dostosowaniu się miasta do współczesnych realiów. Przedstawiłem rozwiązania, które nie naruszają praw obywatelskich do zachowania prywatności, a wspomagają zachowanie zasad bezpieczeństwa w czasach, które uświadamiają nam, że musimy wspólnymi siłami przygotować się na nieoczekiwane scenariusze związane z pandemią.

Detekcja tłumu i kontrola przepływu ludzi Polska, lider technologii związanych z dronami, pokazuje obecnie, jak perspektywiczne jest lotnictwo bezzałogowe. Dziś drony z dużą skutecznością monitorują przestrzeń miejską. Gdy np. wykryją skupiska ludzi nieprzestrzegających zakazu zgromadzeń, przekazują komunikat dźwiękowy, a w razie braku reakcji na miejsce jest wysyłany patrol. Na takie rozwiązanie decyduje się coraz więcej miast, m.in. Siemianowice Śląskie i Śląskie Wojkowice. Pomysłem niezwiązanym z monitoringiem, a godnym uwagi jest transport dronem próbek medycznych i innych materiałów między szpitalami¹⁾, co zmniejsza ry-

zyko infekcji. W Warszawie 29 kwietnia taki lot odbył się pomiędzy szpitalem MSWiA a Centralnym Szpitalem Klinicznym UCK WUM²⁾. System monitoringu wizyjnego miasta pozwala obecnie nie tylko na rejestrację obrazu, ale także analizę różnych elementów otoczenia poprzez zaawansowane funkcje analityczne wbudowane w niektóre modele kamer. Jedną z nich jest zliczanie osób np. w celu detekcji tłumu, kontroli przepływu ludzi, określenia, ile osób weszło do budynku lub ilu klientów przebywa w środku. Możliwa jest także kontrola liczby osób oczekujących w kolejce. Można użyć tych algorytmów w obiektach użyteczności publicznej, sklepach, aptekach, szpitalach. Ciekawym rozwiązaniem jest zastosowanie przez zespół Newcastle Urban Observatory algorytmu, który automatycznie mierzy dystans między pieszymi w miejscach publicznych. Moim zdaniem z powodzeniem można je zastosować w kamerach CCTV.

Monitoring temperatury ciała

Bezkontaktowy system monitorowania temperatury ciała ma na celu zmniejszenie rozprzestrzeniania się epidemii wywołanych przez wirusy, np. COVID-19, świąrska grypa czy inne infekcje wirusowe objawiające się podwyższoną temperaturą. Jest oparty na odpowiednio przystosowanej do pomiaru temperatury człowieka kamerze termowizyjnej i wzorcu temperatury – tylko taki zestaw gwarantuje wysoką dokładność pomiaru, ponieważ przy zmieniających się warunkach termicznych w takich miejscach, jak przeszkłone pomieszczenia czy bezpośrednie wejścia do budynków nie jesteśmy w stanie wykonać skutecznego pomiaru temperatury bez punktu odniesienia. Rozwiązania pozbawione wzorca temperatury narażają użytkownika na błędny pomiar, co może skutkować wpuszczeniem osoby chorej lub generowaniem fałszywych alarmów związanych z detekcją podwyższonej temperatury u osoby zdrowej. Zestaw doskonale sprawdzi się w miejscach o dużym natężeniu ruchu (urzędy, szpitale, szkoły, fabryki, galerie handlowe).

Informowanie o zagrożeniach

Niedocenianym jeszcze rozwiązaniem jest skuteczne i szybkie przekazywanie informacji o zagrożeniu do jak największej liczby mieszkańców za pomocą otaczających nas na każdym kroku wyświetlaczy wizyjnych i kamer z wbudowanymi głośnikami. Powinny być wprowadzone regulacje krajowe w tym zakresie, aby można było z nich korzystać w czasie zagrożenia lub prewencji. Uświadamianie ludzi o skutkach epidemii oraz skuteczna informacja o zbliżającym się zagrożeniu (np. pożarze, powodzi) może uratować wiele istnień ludzkich.

1) <https://www.portalsamorzadowy.pl/wydarzenia-lokalne/samorzadowcy-siegaja-po-drony-w-walce-z-koronawirusem.165596.html>
2) <https://www.tvp.info/47801867/warszawa-dron-dostarczy-probki-do-badan-na-obecnosc-koronawirusa>



Norbert Bartkowiak

Ela-compil

Nowe wyzwania w czasach pandemii

Rozwiązania, którymi możemy zdalnie zarządzać, doceniamy szczególnie w czasach zagrożenia epidemiologicznego. Obecny kryzys związany z pandemią utrudnił życie wielu z nas, ograniczając zwłaszcza możliwość przemieszczania się. Korzystając ze zdalnych systemów do integracji czy sterowania systemami przeciwo-

żarowymi, możemy na odległość swobodnie zarządzać budynkiem. Mając wcześniej odpowiednio skonfigurowane i zintegrowane instalacje, obiekt jest łatwy do administrowania z dowolnego miejsca. Nie ma potrzeby, aby operator był przypisany do konkretnej lokalizacji, gdyż może sterować ustawieniami na odległość.

Wielu zarządców budynków biurowych i centrów handlowych wykorzystало wielotygodniową izolację na przeprowadzenie napraw i remontów. Była to też okazja do testów scenariuszy pożarowych, zwłaszcza tych, których na co dzień nie można przeprowadzić bez wprowadzenia zamieszania w funkcjonującym obiekcie. Bardzo przydatne okazały się w tym przypadku rozwiązania umożliwiające zdalne nadzorowanie infrastruktury teletechnicznej.

Pandemia postawiła także nowe wyzwanie, jakim jest ochrona przed ewentualnymi zagrożeniami. Pojawily się propozycje rozwiązań m.in. opartych na kamerach termowizyjnych, których zadaniem jest identyfikacja osób z podwyższoną temperaturą. W tym przypadku udaje się nam rozszerzyć zakres integracji systemów telewizji dozorowej o kamery termowizyjne. Z kolei producenci wizyjnych systemów zliczających ludzi wskazują na przydatność tych rozwiązań w miejscach, gdzie został wprowadzony limit osób





mogących przebywać w danej strefie. Każde z nich może być skuteczne już jako samodzielne rozwiązanie. Jednak w ramach zintegrowanego systemu uzyskuje się efekt synergii. Proces identyfikacji, lokalizacji i realizacji procedur związanych z danym zdarzeniem jest wtedy wspierany przez zintegrowany system PSIM. Można w te procesy włączyć również istniejące systemy, np. system kontroli dostępu, w którym niewielkie modyfikacje, np. dodanie funkcji służby, mogą znacząco podnieść efektywność poszczególnych rozwiązań. Innym przykładem związanym z kontrolą dostępu są systemy automatyki drzwiowej oferowane przez nasz koncern Gretsch – Unitas. Dużym zainteresowaniem cieszą się rozwiązania, w których drzwi lub służa otwierają się automatycznie, bez użycia rąk; w tym przypadku wykorzystywane są słowniki. Ogranicza się dzięki temu możliwość zakażenia poprzez dotyknięcie klamek.

Mobilność i bezpieczeństwo to aspekty, które obecnie są w naszej branży najważniejsze. Oferowane przez firmę Ela-compil rozwiązania, zarówno GEMOS adv. PSIM, jak i FPM+ są najlepszym przykładem na zwiększenie komfortu pracy i możliwość sprawowania zdalnego nadzoru nad systemami bezpieczeństwa zainstalowanymi w obiektach.



Artur Wądołowski

Hikvision Poland

Oferta security do walki z pandemią

Utrzymujący się stan pandemii sparaliżował niemal wszystkie dziedziny życia. Wymóg noszenia masek ochronnych, częstej dezynfekcji czy zachowania dystansu osobistego utrudnia większości z nas wykonywanie codziennych czynności. W sposób szczególny wymusił zmianę zachowania pracowników różnych organizacji. W dobrej sytuacji

są pracownicy nowoczesnych budynków i biurowców, które już wcześniej wyposażono w systemy tzw. inteligentnego budynku. Wprawdzie nie były to dotychczas urządzenia przeznaczone typowo do przeciwdziałania rozprzestrzenianiu się wirusa, ale zarządzający są w stanie w prosty sposób rozbudować je o dodatkowe elementy i tym samym znacząco zwiększyć poziom bezpieczeństwa w budynku.

Najwięksi światowi producenci systemów zabezpieczeń błyskawicznie wzbogacili swoją ofertę o produkty wspomagające tego typu ochronę. Dobrym przykładem jest firma Hikvision. Producent dostarcza szeroką gamę kamer termowizyjnych i paneli do pomiaru temperatury ciała. Urządzenia te z łatwością współpracują z istniejącymi systemami kontroli dostępu, ograniczając dostęp osób mających podwyższoną temperaturę. Mechanizmy analityki obrazu zapręgnięto do wykrywania obecności masek ochronnych, uniemożliwiając wejście do obiektu osobom bez takiego elementu ochronnego lub przypominając pracownikom o konieczności ich założenia.

Wspomagają pracowników ochrony w liczeniu wchodzących do budynku, aby została zachowana odpowiednia proporcja liczby osób przypadających na powierzchnię dostępną w obiekcie. Kamery z wbudowaną analityką są również w stanie sygnalizować zbyt duże zagęszczenie ludzi i sytuację niezachowywania założonego odstępu pomiędzy osobami. Zatem śmiało można stwierdzić, że w przypadku wielu obiektów stan pandemii przyczynił się do modernizacji zainstalowanych w nich systemów inteligentnego budynku.

Zaczynający się proces wznowienia działalności firm, który prawdopodobnie będzie



trwał kilka najbliższych miesięcy, spowoduje, że w przypadku wielu nowoczesnych obiektów modernizacja istniejących systemów ochronnych pod kątem zwiększenia bezpieczeństwa medycznego wkrótce nabierze większego tempa.



Tomasz Kowalewski

Ezviz

Trudne czasy dla smart home?

Zastosowanie urządzeń i systemów inteligentnego domu z założenia nie miało na celu wyłącznie zabezpieczania mienia czy monitorowania osób – łączą one płynnie koncepcję zapewnienia bezpieczeństwa i komfortu w przystępnej, intuicyjnej formie. Na ich coraz większą powszechność wpływa łatwość montażu i użytkowania. Popularność rozwiązań smart home jest silnie determinowana przez ich przydatność do różnego rodzaju zastosowań, które coraz bardziej wykraczają poza aspekty zabezpieczenia i częściej stanowią o codziennej wygodzie i szeroko rozumianym bezpieczeństwie rodziny czy domowników.

W czasach pandemii produkty smart home mogą okazać się niezwykle pomocne w różnych sytuacjach. Biorąc pod uwagę opiekę na seniorami, obecnie szczególnie narażonymi, kamery Wi-Fi z dwukierunkowym torem audio i dostępem z poziomu smartfona są nieocenione, zapewniając komunikację głosową i wizualną na odległość, np. w razie koniecznej pomocy czy zrobienia zakupów, bez niepotrzebnego narażania na zbyt częsty kontakt osobisty. Warto również rozważyć kamery z komunikacją Wi-Fi w kontekście ochrony seniorów przed oszustami podszywającymi się pod rozmaitych funkcjonariuszy właśnie w dobie pandemii. Brak Wi-Fi nie jest przeszkodą, gdyż oferowane są także kamery z komunikacją 4G LTE.

Pandemia przyczyniła się do dużego wzrostu zakupów online, stąd jednym z częstszych gości jest kurier czy listonosz. Dzięki zamontowanemu wizjerowi drzwiowemu lub bramowemu czy choćby

kamerze z dwukierunkowym torem audio, możemy ograniczyć kontakt z osobą bardziej narażoną na kontakt z wirusem. Wizjer drzwiowy lub kamera umożliwią rozmowę z kurierem z poziomu smartfona, gdy akurat nie ma nas w domu, i pozostawienie przesyłki we wskazanym miejscu. Kamery C4W ze spersonalizowanymi alertami głosowymi mogą okazać się odsieczą dla właścicieli małych biznesów. Kamera ta może, w momencie detekcji ruchu, rozgłaszać komunikaty, np. o maksymalnej liczbie osób mogących znajdować się w sklepie czy konieczności dezynfekcji rąk przed wejściem, a w godzinach zamknięcia sklepu realizować typową funkcję monitoringu wizyjnego.

Kluczową funkcjonalnością systemów smart home, przekładającą się na wygodę i bezpieczeństwo w okresie pandemii, jest więc umożliwienie pozostania w zdalnym kontakcie głosowym i wizualnym z osobami izolowanymi, przebywającymi na kwarantannie, pod opieką czy chcącymi ograniczyć ryzykowne kontakty. Kolejne możliwości poprawy bezpieczeństwa odsłaniają spersonalizowane komunikaty głosowe.



Jakub Sobek

Linc Polska

FIZYKA równa dla wszystkich?

Pomiar temperatury, mierzenie temperatury, badania przesiewowe temperatury... W mediach aż huczy od informacji o sposobach walki z wirusem. Oczywiście badania profilaktyczne są bardzo istotne. Wszystkim powinno zależeć na ograniczeniu rozprzestrzeniania się epidemii, z tym nie należy dyskutować. Jednak ze zdziwieniem obserwowałem rewelacje prezentowane przez poszczególnych producentów oraz to, na jaki zakup decydowali się klienci końcowi. Można odnieść wrażenie, że w przypadku niektórych rozwiązań prawa fizyki przestały obowiązywać. Okazywało się, że niektóre kamery termowizyjne potrafią mierzyć temperaturę w każdych

warunkach na praktycznie dowolnym dystansie. Rzeczowa i techniczna wiedza została odłożona na bok, a wraz z nią etyka, niestety. Wszystko na rzecz przekonania do własnego produktu za wszelką cenę. Inwestorzy czasem w takie zapewnienia wierzą, a czasem chcą wierzyć. Decydują się przy tym na rozwiązania, które dają tylko pozorne rozwiązanie problemu. Nie wolno jednak zapominać, że na szali leży zdrowie, a nawet życie wielu osób.

Czy zatem pomiar powierzchniowy temperatury ludzkiego ciała za pomocą kamer termowizyjnych ma sens? Oczywiście, ma! Pod warunkiem, że jest przeprowadzany w odpowiedni i bezpieczny sposób. Olbrzymią zaletą termowizji jest pomiar bezkontaktowy, prowadzony automatycznie z pewnej odległości. To pozwala odciążyć pracownika ochrony od dokonywania pomiarów za pomocą klasycznego termometru zbliżeniowego. W ten sposób minimalizujemy też ekspozycję pracownika na kontakt z innymi osobami. Już w trakcie epidemii wywołanej przez SARS kamery termowizyjne udowodniły swoją skuteczność na lotniskach azjatyckich, są to rozwiązania sprawdzone w realnym działaniu.

Jeśli technologia termowizyjna zostanie rozpowszechniona i będzie stosowana w sposób prawidłowy, stanie się bardzo przydatnym narzędziem. Może przyczynić się do szybszego opanowania epidemii. Natomiast w kolejnym etapie będzie istotnym elementem profilaktycznym, który pozostanie z nami na długo, a nawet stanie się obowiązującym standardem.

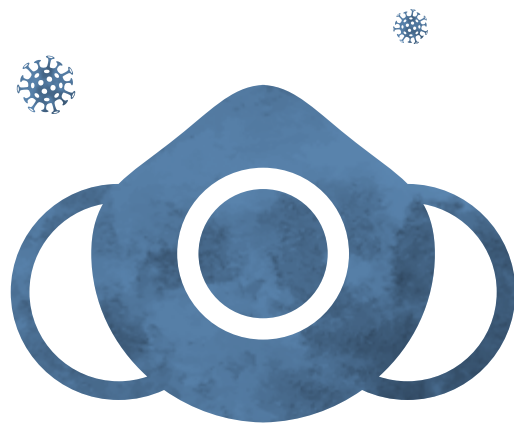


Angelika Prokop-Grey

ASIS International Poland Chapter

Bezpieczeństwo mieszkańców miast w czasie pandemii

Panująca obecnie pandemia koronawirusa, dotykająca szczególnie gęsto zaludnione re-



jony świata, pokazuje niestety, że przeciwdziałania podejmowane przez władze państwowe i lokalne oraz oficjalne organizacje nie przynoszą dostatecznych rezultatów.

Są pozytywne wyjątki: Tajwan, Singapur i Korea Południowa po doświadczeniach z wirusem SARS w 2002 r. dobrze przygotowały się na ryzyko kolejnej pandemii. Niestety reszta świata zignorowała sygnały naukowców ostrzegających przed katastrofą. Brak sprzętu medycznego, brak miejsc w szpitalach na wypadek większej liczby chorych – nie były przykładami nieprzewidzianego ryzyka, lecz słabego zarządzania.

Miasta o wysokiej skali przestępczości zorganizowanej, np. Rio de Janeiro, doświadczyły wręcz przejęcia inicjatywy przez grupy przestępcze. Skoro mieszkańcy nie przestrzegali wprowadzonych zasad, np. godziny policyjnej, członkowie gangów wzięli sprawy w swoje ręce i jeżdżąc po ulicach, nawoływali mieszkańców do pozostania w domu, często strasząc bronią.

Przekonanie, że silna policja gwarantuje bezpieczeństwo w mieście, już dawno odeszło do lamusa. Dziś jest to bowiem suma wielu elementów, takich jak kompetencje osób zarządzających, wysoki poziom służb bezpieczeństwa, stosowanie nowoczesnych technologii, współpraca z sektorem prywatnym, dzielenie się doświadczeniami z innymi miastami w kraju i za granicą, a także świadomość obywateli (zaangażowanie, przestrzeganie reguł, odpowiedzialność za dobro wspólne). Branża security ma odpowiednie zasoby, duże doświadczenie i nowoczesne technologie niezbędne do budowy miejskich systemów bezpieczeństwa. Wspomniane już władze Tajwanu, Korei Południowej czy miasta-parostwa Singapur od lat współpracują z sektorem prywatnym. Zastosowanie technologii big data i AI w budowanych tam systemach stało się powszechne. Zaproszenie ekspertów ds. bezpieczeństwa przez władze lokalne do współpracy przy budowie nowych systemów i technologii zwiększających bezpieczeństwo nas wszystkich wydaje się więc jedyną drogą. ▣



RODO A SYSTEMY KONTROLI DOSTĘPU

Cz.1. Biometria w zatrudnieniu

ADMINISTRATORZY DANYCH OSOBOWYCH MUSZĄ MIEĆ ŚWIADOMOŚĆ, ŻE PRZETWARZANIE DANYCH BIOMETRYCZNYCH WIĄŻE SIĘ NIE TYLKO Z DUŻYM RYZYKIEM DLA PODMIOTU DANYCH, ALE I WIZERUNKOWYM DLA NICH SAMYCH W PRZYPADKU NARUSZENIA DANYCH. TRZEBA TEŻ ZNAĆ WYMAGANIA RODO ZE WZGLĘDU NA PRZETWARZANIE SZCZEGÓLNYCH KATEGORII DANYCH.



T E K S T
Piotr Powązka

Wykorzystanie w systemach kontroli dostępu danych biometrycznych (odciski palców, tęczę oka, układ żył) jako danych identyfikujących osobę zatrudnioną zyskuje wśród pracodawców na popularności – wydaje się szybkim i nowoczesnym rozwiązaniem w zakresie zapewnienia bezpieczeństwa lub zapobiegania nadużyciom. Postrzegana akceptację danych biometrycznych zwiększyło ich wykorzystanie do użytku osobistego (np. w celu korzystania z funkcji smartfonów, ewidencji czasu pracy czy dostępu do placówek użyteczności publicznej, np. siłowni). Tradycyjna niechęć do systemów biometrycznych była i pozostaje związana z ochroną praw osób. Nowe systemy i ich rozwój budzi wiele obaw. Dotyczą one m.in. możliwości niejawnego gromadzenia, przechowywania i przetwarzania materiału zawierającego informacje szczególnie chronione, a te czynności mogą naruszyć najintymniejsze sfery prywatności osób fizycznych.

Od początku stosowania technologii i systemów biometrycznych poważny problem stanowi potencjalne ich nadużywanie. Wraz z rosnącym potencjałem technicznym nowych systemów (dotyczy to zwłaszcza rozpoznawania twarzy) ryzyko wykorzystywania danych w sposób niezgodny z ich pierwotnym celem rośnie. Stosowanie takich technologii musi odbywać się z należytym poszanowaniem zasad legalności, konieczności, proporcjonalności i minimalizacji danych, określonych w RODO. Mimo że korzystanie z tych technologii może być postrzegane jako szczególnie skuteczne, administratorzy powinni ocenić ich wpływ na podstawowe prawa i wolności oraz rozważyć zastosowanie mniej „inwazyjnych” środków do osiągnięcia legalnego celu ich przetwarzania.

KONIECZNE ELEMENTY BIOMETRII

Aby mówić o przetwarzaniu danych biometrycznych, muszą być spełnione następujące warunki:

- dane dotyczą osoby fizycznej,
- umożliwiają jednoznaczne zidentyfikowanie tej osoby (samodzielnie lub w powiązaniu z innymi informacjami),
- stosowane jest adekwatne przetwarzanie techniczne.

Nie ma przy tym znaczenia, że ani czytnik linii papilarnych, ani skaner źrenicy oka nie zapisują wzoru daktyloskopijnego, a wynikiem pomiaru/skanu jest zapis cyfrowy, stanowiący jakąś sumę kontrolną. Nie jest przy tym istotne, że z tego zapisu matematycznego nie można odtworzyć odcisku palca czy skanu źrenicy.

W swoim artykule nt. stosowania monitoringu wizyjnego w nr. 6/2019 poruszyłem kwestie kluczowych zasad RODO oraz wymogów, jak badanie NIEZBĘDNOŚCI, PROPORCJONALNOŚCI I LEGALNOŚCI (art. 5 RODO) czy analizy ryzyka i uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, o których mowa w art. 25 RODO. Mają one zastosowanie również w przypadku stosowania roz-

Przetwarzanie danych biometrycznych podlega sztywnym przepisom prawa o ochronie danych osobowych, trudnych do przestrzegania w kontekście zatrudnienia, ale i stosowania w przypadku rozwiązań konsumenckich czy w sferze publicznej

wizań biometrycznych w kontroli dostępu. Przywołane poprzednio wytyczne EROD wywołały wiele dyskusji, wątpliwości i nowego spojrzenia nt. monitoringu również przez rodzime UODO. Warto zatem śledzić rozwój wydarzeń, gdyż UODO już zapowiada aktualizację swoich zaleceń dla administratorów, w tym prawdopodobnie inne podejście do podglądu obrazów z kamer na żywo bez zwyczajowej rejestracji na nośniku danych.

BIOMETRIA A KWESTIE PRACOWNICZE

W kwestiach pracowniczych polskie i zagraniczne regulacje Kodeksu pracy (KP) w niektórych przypadkach przewidują możliwość stosowania biometrii. Art. 22(1b) „Przetwarzanie danych biometrycznych ubiegającego się o pracę lub pracownika” stanowi:

- § 1.** Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 przetwarzanie szczególnych kategorii danych osobowych ust. 1 rozporządzenia 2016/679, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Przepis art. 221a zgoda ubiegającego się o zatrudnienie lub pracownika na przetwarzanie danych § 2 stosuje się odpowiednio.
- § 2.** Przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.
- § 3.** Do przetwarzania danych osobowych, o których mowa w § 1, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Wymóg, aby administratorzy danych będący pracodawcami wdrażali odpowiednie środki techniczne i organizacyjne (art. 32 ust. 1 RODO) nie oznacza, że pracodawca od razu wdroży system kontroli dostępu i ewidencji czasu pracy z identyfikacją biometryczną. Trzeba bardzo ostrożnie podchodzić do wymogów prawnych i zagrożeń oraz skrupulatnie stosować zasady ochrony danych w tym zakresie. Urząd Ochrony Danych Osobowych w swoim poradniku dotyczącym zatrudnienia opublikowanym w 2018 r. kategori- 



→ dencji czasu pracy. Z moich doświadczeń wynika, że niektórzy pracodawcy decydują się na takie rozwiązania wbrew obowiązującym przepisom. Już 11 lat temu, a zatem jeszcze w czasach dyrektywy 95/46/WE, kiedy dane biometryczne nie były uważane za szczególne dane osobowe, NSA w wyroku z 1 grudnia 2009 r. (sygn. I OSK 249/09) orzekł:

Brak równowagi w relacji pracodawca – pracownik stawia pod znakiem zapytania dobrowolność wyrażenia zgody na pobieranie i przetwarzanie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 22 Kodeksu pracy katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 22 Kodeksu pracy stanowiłoby obejście tego przepisu.

– Ryzyko naruszenia swobód i fundamentalnych praw obywatelskich musi być proporcjonalne do celu, któremu służy. Skoro zasada proporcjonalności jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania.[...]

Pracodawcy na swoją obronę podnoszą kwestie nadużyć pracowników, polegających na potwierdzaniu obecności osób przez kolegów, co naraża firmy na straty i inne zagrożenia. Próbuje również przy okazji ewidencji sprawdzać, poprzez monitoring wizyjny, autoryzujących się w czytniku pracowników. Jednak tu również często występuje problem z zasadą proporcjonalności.

Nawet wyraźna zgoda zazwyczaj nie może być uznana za legalną podstawę przetwarzania danych biometrycznych osób w miejscach pracy. Uzyskanie ważnej (dobrowolnie wyrażonej) zgody zatrudnionego jest na ogół trudne ze względu na nieodłączny związek z podporządkowaniem się pracownika względem pracodawcy, a więc nierównowagi sił. Ponadto, zakładając, że pracownicy rzeczywiście mogliby swobodnie wyrażać zgodę (lub nie wyrażać jej), sytuacja, że pewien odsetek pracowników nie wyraża zgody na przetwarzanie ich danych biometrycznych, zazwyczaj nie pozwala pracodawcy na osiągnięcie zamierzonego celu (nawet gdy środek jest uzasadniony względami bezpieczeństwa, ważne jest, aby miał akceptację wszystkich pracowników).

UODO w swoim poradniku dot. zatrudnienia z 2018 r. kategorycznie zabronił stosowania biometrii w zakresie ewidencji czasu pracy



W pierwszej kolejności pracodawca powinien zastanowić się nad alternatywnymi środkami, które nie wymagają przetwarzania danych biometrycznych, a pozwalają osiągnąć ten sam cel w sposób mniej kontrowersyjny (tzn. są odpowiedniejsze). Powinien zdecydowanie rozważyć połączenie różnych mniej inwazyjnych rozwiązań, np. osobistego kodu dostępu i osobistego identyfikatora np. do zabezpieczenia dostępu do systemu kasowego sklepu przed kradzieżą. Ponieważ nie zawsze jest to łatwe zadanie, zaleca się dokładne udokumentowanie tej oceny, jej uzasadnienia i wyniku.

Jeżeli przetwarzanie danych biometrycznych nadal wydaje się bardziej odpowiednie do osiągnięcia zamierzonego celu, pracodawca musi dokładnie ocenić jego legalność zgodnie z art. 6 i 9.2. RODO. Przykładem może być tu kontrola dostępu do niektórych pomieszczeń czy elementów infrastruktury krytycznej, dla której analiza wykaże niezbędność dodatkowej ochrony dostępu.

Artykuł 9 ust. 2. RODO zawiera inne wyjątki, które pozwalają na przetwarzanie danych biometrycznych, a pracodawca powinien sprawdzić, czy któryś z nich może zastosować. Gdy brak wyjątków na mocy art. 9 ust. 2 lub prawa krajowego dotyczącego ochrony danych osobowych, zgoda zatrudnionego może wydawać się jedyną opcją dla pracodawcy. W ograniczonych przypadkach można opierać się na zgodzie jako na legalnej podstawie, pod warunkiem że pracodawca zaoferuje pracownikom alternatywne rozwiązania i wiarygodną gwarancję, że nie wystąpią działania odwetowe w razie niewyrażenia zgody. Jeżeli pracownicy czują się w jakikolwiek sposób zmuszeni do wyrażenia zgody, nie będzie ona ważna i w konsekwencji przetwarzanie danych będzie niezgodne z prawem.

– Naruszenie przepisów ochrony danych przez pracodawcę w Holandii

W Holandii zapadł w 2019 r. wyrok sądu w sprawie pracodawcy, który wprowadził oparty na odciskach palców system autoryzacji, pozwalający kontrolować dostęp pracowników do systemu kasowego. Zastąpił on poprzedni system kontroli dostępu (KD) oparty na osobistym kodzie dostępu. Pracodawca ogłosił, że ma ku temu przesłanki:

- musi zapobiegać oszustwom i kradzieżom przez pracowników,
- musi chronić wrażliwe dane dostępne za pośrednictwem systemu kasierskiego (tj. dane finansowe i dane osobowe pracowników i klientów).

Później do systemu KD dodał inną funkcjonalność – rejestrację czasu pracy. Argumentował, że jako administrator danych jest zobowiązany do wdrożenia odpowiednich środków technicznych i organizacyjnych (zgodnie z art. 32 ust. 1 RODO). W tym względzie uznano, że poprzedni system oparty na kodach osobowych nie jest już odpowiedni w obecnych czasach i istnieje ryzyko, że może zostać ominięty lub zhakowany. Ponadto pracodawca stwierdził, że korzystanie z danych biometrycznych staje się powszechnie akceptowane i że są one szeroko stosowane, np. w celu uzyskania dostępu do funkcji smartfonów. W tej sytuacji pracownik odmówił podania swoich odcisków palców, twierdząc, że narzucony system narusza jego prawa do ochrony danych osobowych.

DECYZJA SĄDU: w rozpatrywanej sprawie przetwarzanie danych biometrycznych pracowników zostało narzucone jednostronnie (pracownicy nie mieli wyboru), więc nie można było powoływać się na zgodę jako na legalną podstawę. Nie można było również powołać się na krajowy wyjątek w nietherlandzkiej ustawie o ochronie danych, tj. gdy przetwarzanie jest konieczne do celów uwierzytelnienia lub bezpieczeństwa:

- interes przedsiębiorstwa (tj. zapobieganie oszustwom i kradzieżom przez pracowników) nie stanowi przesłanki „niezbędnej do celów uwierzytelniania” (tu sąd odniósł się do przykładu elektrowni jądrowych jako elementów infrastruktury krytycznej i zagrożeń z tym związanych),
- przetwarzanie nie jest proporcjonalne, ponieważ w sklepie nie były zainstalowane inne zabezpieczenia, tzn. nie było systemów alarmowych, nie było seifu ani nadzoru kamer,
- pracodawca nie wykazał w wystarczającym stopniu, dlaczego nie uwzględniono innych, mniej naruszających prywatność identyfikatorów, np. połączenia karty i kodu osobistego.

Sąd orzekł, że pracodawca nie może narzucić systemu autoryzacji opartego na odciskach palców, ponieważ w danych okolicznościach narusza to przepisy RODO i holenderską ustawę o ochronie danych.

Holenderski urząd ochrony danych, *Autoriteit Persoonsgegevens*, nałożył na inne przedsiębiorstwo grzywnę w wysokości aż 725 tys. euro za naruszenie ogólnego rozporządzenia UE o ochronie danych. Organ ochrony danych stwierdził, że nienazwana firma wymagała od swoich pracowników skanowania odcisków palców w celu sprawdzania ich obecności, a więc prowadzenia ewidencji czasu pracy. W tym przypadku, takie wykorzystanie informacji biometrycznych nie spełnia wymogów określonych w rozporządzeniu o ochronie danych osobowych.

– Kara UODO nałożona na szkołę za stosowanie biometrii w stołówce

Prezes UODO nałożył karę finansową w wysokości 20 tys. zł na Szkołę Podstawową nr 2 w Gdańsku za niezgodne z prawem przetwarzanie danych biometrycznych. (Maksymalna wysokość kary, jaką można nałożyć na podmiot publiczny zgodnie z ograniczeniem, jakie przewiduje krajowa Ustawa o Ochronie Danych Osobowych z 10 maja 2018 r., to 100 tys. zł) UODO w swej decyzji z 18 lutego 2020 r. stwierdza:

Należy zauważyć, iż przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Wyżej wymienioną identyfikację Szkoła może przeprowadzić za pomocą innych środków, mniej ingerujących w prywatność dziecka korzystającego z usług stołówki szkolnej.

[...] Zgodnie z zasadami wydawania obiadów umieszczonymi na stronie stołówki prowadzonej przez Szkołę – uczniowie, którzy nie posiadają identyfikacji biometrycznej, przepuszczają wszystkich i oczekują na końcu kolejki (pkt 3), oraz gdy wszyscy uczniowie z identyfikacją biometryczną wejdą do stołówki, rozpoczyna się wpuszczanie pojedynczo uczniów bez identyfikacji biometrycznej [...] To przejaw dyskryminacji.

[...] Realizując tę usługę, Szkoła może przetwarzać tylko te dane osobowe ucznia, które są niezbędne do świadczenia usług stołówki szkolnej. Wskazać należy, że przepisy prawa powszechnie obowiązującego wskazują rodzaj danych, jakie Szkoła może pozyskiwać od swoich uczniów. Żaden z nich nie zezwala Szkole na przetwarzanie (pozyskiwanie i gromadzenie) danych biometrycznych (których przetwarzanie jest co do zasady zakazane w art. 9 ust. 1 RODO) uczniów w celu realizacji tego zadania.

W takiej sytuacji zgoda Rodzica nie może być przesłanką legalizującą przetwarzanie danych biometrycznych, ponieważ zgoda stanowi podstawę legalizującą przetwarzanie danych osobowych jedynie wtedy, gdy nie istnieją inne przesłanki na te przetwarzanie. [...]

Szkoła wyszła z założenia, że nie zbiera danych biometrycznych. Patrząc jednak na KONIECZNE ELEMENTY BIOMETRII wspomniane wyżej, była to błędna teza:

- specjalne rozwiązanie techniczne, czyli skaner odcisków palca, przetworzył dane w sposób matematyczny.
- jest możliwość zidentyfikowania osoby fizycznej i porównanie w bazie danych.

Identyczne zdanie miał organ w Szwecji, przy czym tam sprawa dotyczyła rozpoznawania twarzy i obecności dzieci.

Przetwarzania danych biometrycznych nie można traktować po-błażliwie, zwłaszcza w kontekście zatrudnienia czy szkolnictwa, gdzie ważna zgoda pracownika nie jest zazwyczaj dobrym rozwiązaniem. Wraz z rozwojem technologii i np. umieszczaniem odcisków palców podczas identyfikacji elektronicznej jest to prawdopodobnie jedynie wierzchołek góry lodowej problemów. Zapewne będziemy świadkami wielu innych przypadków wykorzystywania lub utraty danych biometrycznych oraz wytycznych w tym zakresie. ▣

ERATRUST
ul. Postępu 10/34,
02-676 Warszawa
biuro@eratrust.pl

B I O

Piotr Powązka

Absolwent Uniwersytetu Ekonomicznego we Wrocławiu. Ma kilkunastoletnie doświadczenie korporacyjne w sektorach finansowym i technologicznym. Zaangażowany w kształtowanie prywatności i praktyk handlowych poprzez budowanie zrównoważonej wartości biznesowej, propaguje nowe standardy w umowach oraz kulturę ery zaufania i współpracy. Wspiera organizacje w zakresie transformacji cyfrowej, ochrony danych osobowych i prywatności, zarządzania kontraktami, zgodności i kontroli wewnętrznej oraz modelowania procesów biznesowych. Jego publikacje obejmują m.in. tematy cen transferowych, kryptowalut, smart contracts, ochronę danych osobowych czy zarządzanie umowami. Członek The International Association of Privacy Professionals (IAPP) oraz Członek Rady The International Association for Contract & Commercial Management.



Coś się kończy, coś się zaczyna

Finał sukcesji w Schrack Seconet Polska



W połowie ub. roku firma Schrack Seconet Polska poinformowała branżę o zmianach w Zarządzie spółki przewidywanych na pierwszą połowę 2020 r. Prezes Zarządu firmy – Grzegorz Ćwiek – podjął wiosną 2019 r. decyzję o rezygnacji z pełnionej funkcji i zmianie swojej ścieżki rozwoju zawodowego, wdrażając jednocześnie przemyślane i uzgodnione z Radą Nadzorczą plan sukcesji, tak by decyzja ta nie zaburzyła dotychczasowego zrównoważonego rozwoju przedsiębiorstwa. Z dniem 1 maja 2020 stanowisko Prezesa Zarządu Schrack Seconet Polska Sp. z o. o. objął Michał Sidor, związany z firmą od 11 lat, a od 2014 r. zajmujący stanowisko dyrektora handlowego w Polsce.



SZANOWNI PAŃSTWO,

realizacja trwającego od ponad roku planu mojej sukcesji dobiegła właśnie końca. W ostatnim dniu kwietnia tego roku miałem przyjemność przekazać mojemu wieloletniemu współpracownikowi i skutecznemu menedżerowi – Michałowi Sidorowi – obowiązki Prezesa Zarządu Spółki, której byłem częścią od ponad 20 lat. Przy tej okazji chciałbym wszystkim gorąco podziękować za cały ten wspólny czas wspólnej pracy, nauki, zabawy, zdobywania doświadczeń życiowych i zawodowych, a przede wszystkim – piękną część życia, którą z Wami spędziłem. Żywię wielką nadzieję, że pełniąc funkcję lidera wspianego Zespołu, który pozostawiam pod opieką nowego zarządu, zaznaczyłem swoją obecność w Państwa życiu zawodowym w sposób wartościowy i wniosłem do Waszych doświadczeń wiele pozytywnej energii, dobrych emocji, a także wiedzy z zakresu bezpieczeństwa pożarowego, systemów zintegrowanych czy zasad budowy organizacji odpornych na zakłócenia i kryzysy.

W moim wieloletnim doświadczeniu na stanowiskach menedżerskich, aż po funkcję członka zarządu, doświadczyłem kilku poważnych kryzysów rynkowych i zagrożeń ciągłości działania krytycznych procesów, jednak zawsze dokonywaliśmy niemożliwego, osiągając sukces i wzrost wbrew koniunkturze i lokalnym czy międzynarodowym turbulencjom rynkowym. Z całego serca życzę mojemu następcy, by wraz z dojrzałym i niezwykle doświadczone Zespołem dokonywał jeszcze bardziej spektakularnych „cudów” i kontynuował wszystkie dobre praktyki, które wypracowaliśmy na przestrzeni wielu lat działalności w firmie – począwszy od jej powstania, poprzez sukcesy moich poprzedników i mój wkład, aż do tej chwili, kiedy to mimo globalnej pandemii osiągamy najlepsze wyniki działalności w historii firmy. Staram się nie podejmować ważnych dla mnie decyzji życiowych, wobec których nie czuję dreszczu ekscytacji. Tak właśnie jest teraz, kiedy, odchodząc z Zarządu Spółki, kieruję swoje życie na nową ścieżkę rozwoju. Zapewniam jednak, że podejmując nowe wyzwania, którym oddaję się z wielkim zapałem – nie pozostawiam moich koleżanek i kolegów, Partnerów biznesowych oraz innych interesariuszy firmy w Polsce bez wsparcia i kontaktu. Przyjmując nowe role i zadania w projektach międzynarodowych, pozostaję nadal do Państwa dyspozycji i z przyjemnością będę dzielił się moimi doświadczeniami, wiedzą i pasjami, a także nadal uczył się od Was – jeżeli tylko uznacie Państwo naszą wspólną podróż w przyszłość za równie pasjonującą.

**Życząc zdrowia, ciepło pozdrawiam,
GRZEGORZ ĆWIEK**



SZANOWNI PAŃSTWO,

jako wieloletni członek spójnego i nieustannie rozwijającego się Zespołu profesjonalistów, miałem okazję towarzyszyć moim koleżankom i kolegom w budowie sukcesu Schrack Seconet w Polsce, pełniąc swoje obowiązki na różnych stanowiskach – począwszy od członka zespołu handlowego, a później jego lidera, by w ostatnim czasie objąć funkcję dyrektora zarządzającego. Zaufanie, jakim obdarzyli mnie pan Grzegorz Ćwiek, opuszczający stanowisko Prezesa Zarządu, oraz właściciel spółki (Schrack Seconet AG), a także wsparcie Zespołu, którego jestem członkiem, motywuje mnie do kontynuowania dobrych praktyk i aktualnej strategii działania firmy w Polsce. Plan sukcesji, w którego finale to właśnie mnie powierzono pełnienie funkcji Prezesa Zarządu, obejmuje też nasze pełne przekonanie o słuszności kontynuowania polityki i strategii rozwoju firmy, przyjętej przez mojego poprzednika w wieloletnim planie rozwoju. Założenie to ma jeszcze większe znaczenie dzisiaj, kiedy to globalna pandemia wywołująca lokalne niepokoje i światowy kryzys gospodarczy wystawia na próbę lojalność producentów wobec Partnerów biznesowych, współpracowników i weryfikuje prawdziwych przyjaciół, w odróżnieniu od tych, którzy, ratując własne interesy, zapominają o tym, co ważne.

Schrack Seconet Polska cieszy się ogromnym zaufaniem wśród swoich Partnerów i użytkowników produktów ze względu na niezachwianą stabilność dotychczasowej filozofii rozwoju, strategii cenowej, jakości technicznej i lojalności w relacjach ze wszystkimi interesariuszami. Moim zadaniem i zarazem największym wyzwaniem w najbliższym czasie będzie utrzymanie tego zaufania i kontynuowanie rozwoju przedsiębiorstwa w Polsce, które osiągnęło pozycję niekwestionowanego lidera wśród dostawców nowoczesniejszych technologii z dziedziny zintegrowanego bezpieczeństwa przeciwpożarowego.

Przedemną, jak i przed całym Zespołem – który niezwykle cenię – wiele zadań i kolejne ciekawe przygody. Dla wielu z nas bowiem realizacja zadań trudnych i nadzwyczajnych to pasja i doświadczenia na miarę wypraw w nieznane. Przecieraliśmy wspólnie szlaki, wprowadzając branżę na nieodkryte dotąd ścieżki rozwoju nowych produktów, dzieliliśmy się z Państwem naszymi pasjami poprzez oryginalne podejście do marketingu oraz prezentowaliśmy odpowiedzialną społecznie postawę producenta i dostawcy usług służących ochronie zdrowia i życia. To wszystko realizowaliśmy dotychczas pod przywództwem naszego wieloletniego przełożonego, kolegi, ale przede wszystkim przyjaciela, któremu pragnę – w imieniu swoim i całego Zespołu – serdecznie podziękować za codzienną pomoc, wsparcie, dzielenie się doświadczeniem i, co najważniejsze, motywację do rozwoju osobistego. Pragnę Państwa zapewnić, że dołożę wszelkich starań, by moja praca na rzecz rozwoju firmy, wspierania naszych współpracowników w ich codziennym działaniu, rozwoju jak najlepszych relacji z naszymi Partnerami, Klientami i środowiskiem branżowym nie zawiodła zaufania wszystkich tych, dla których silna i sprawna organizacja Schrack Seconet w Polsce jest ważna i bliska sercu.

Zapraszam do dalszej współpracy!

MICHAŁ SIDOR,

Prezes Zarządu Schrack Seconet Polska

Mimo panującej na świecie pandemii koronawirusa Schrack Seconet Polska pozostaje w pełnej gotowości do nieprzerwanego działania we wszystkich obszarach swojej aktywności. Pracownicy firmy, zarówno w oddziałach w Polsce, jak i na całym świecie, są do Państwa dyspozycji. Niezmiennie działa też wsparcie techniczne, wraz z uruchomionym w połowie marca cyklem szkoleń online, kierowanych zarówno do projektantów, jak i programistów – wdrożeniowców, serwisantów. Jesteśmy także gotowi do prowadzenia prezentacji indywidualnych na życzenie, w pełnym zakresie produktowym. Aktualna lista szkoleń jest dostępna na dedykowanej do tego stronie: wydarzenia.schrack-seconet.pl

W trosce o zdrowie i bezpieczeństwo naszych Partnerów biznesowych oraz entuzjastów i uczestników organizowanych przez nas wydarzeń, jesteśmy zmuszeni odwołać wszystkie imprezy zaplanowane do końca tego roku, m.in. szkolenia stacjonarne – projektowe i specjalistyczne w regionach, Międzynarodowy Złot Moto-cyklowy Branży Systemów Bezpieczeństwa, Branżowe Spotkanie Kobiet, Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego. Dołożymy wszelkich starań, by w przyszłości zrekomensować wszystkim brak możliwości udziału w tegorocznych spotkaniach. Nasz zespół pracuje obecnie nad kolejnymi projektami online, które pozwolą wesprzeć Państwa w codziennej pracy i choć w ten sposób poprawić Państwu nastrój.



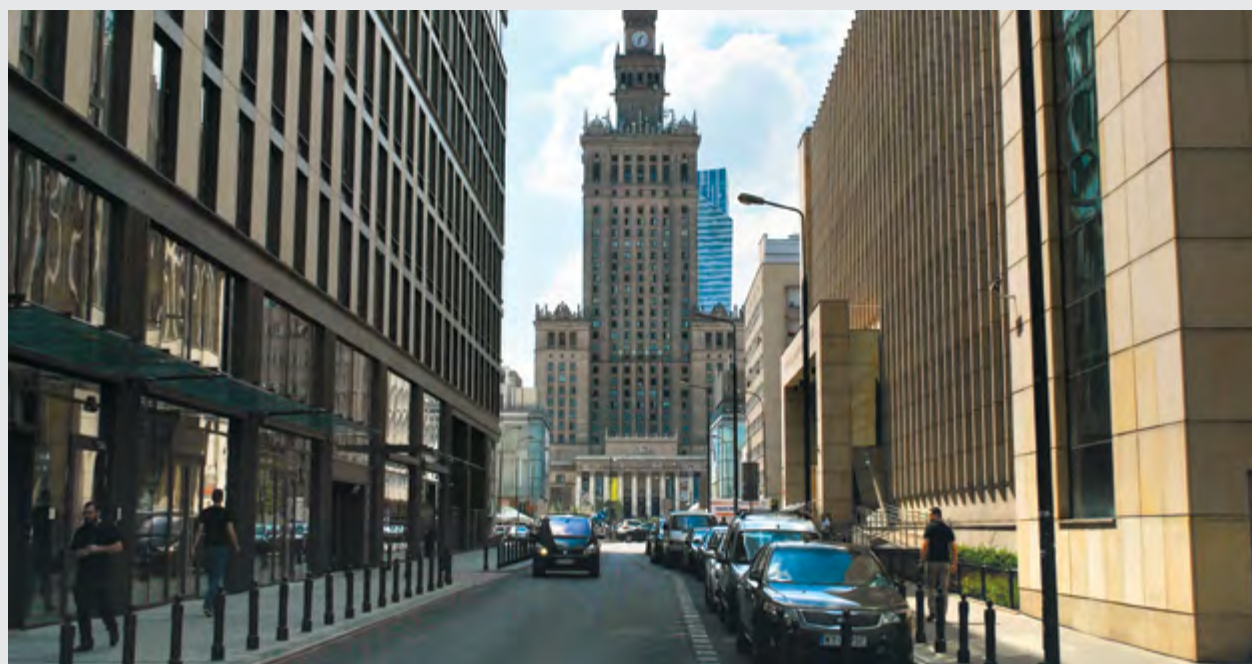
Już w początkowej fazie epidemii błyskawicznie opracowaliśmy specjalną ofertę cenową oraz szkolenia z zakresu narzędzi zdalnego dostępu wchodzących w skład pakietu Integral Remote. Chcieliśmy tym samym ułatwić Państwu oraz właścicielom i użytkownikom obiektów nieprzerwany nadzór nad oferowanymi przez nas systemami bezpieczeństwa, a także bezpieczny powrót do stabilnej i wygodnej codziennej pracy. Gama produktów do zdalnej obsługi Integral Remote zapewnia: stały, nieograniczony dostęp do systemu, błyskawiczną reakcję na zagrożenia bez konieczności dojazdu do serwisowanych obiektów w celu zdiagnozowania problemów, znaczne obniżenie kosztów serwisu, wsparcie bezpieczeństwa Waszych pracowników, ograniczenie liczby osób niezbędnych do nadzorowania systemu oraz wiele innych znaczących korzyści i dla inwestorów, i dla firm serwisujących. Zachęcamy do zapoznania się ze szczegółami oferty i do kontaktu: https://www.schrack-seconet.com/pl/company/news_events/

Zespół Schrack Seconet Polska

Schrack Seconet Polska

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





Wtyczka AXIS Optimizer for Milestone XProtect®

Axis Communications współpracuje z firmą Milestone – światowym liderem w obszarze systemów zarządzania materiałem wizyjnym (VMS). Korzystając z wtyczki AXIS Optimizer for Milestone XProtect®, można sprawnie wyszukiwać zarejestrowany materiał wizyjny dotyczący pojazdów.

Rozwiązanie umożliwia gromadzenie ważnych danych o ruchu drogowym i zarządzanie wszystkimi związanymi z tym aspektami – od automatycznego wykrywania tablic rejestracyjnych pojazdów po informacje niezbędne podczas prac wyjaśniających. Operacje detekcji, rozpoznawania i klasyfikacji pojazdów oraz identyfikacji tablic rejestracyjnych są wykonywane w kamerze (urządzeniu brzegowym sieci), z której trafiają do systemu VMS. Operatorzy systemów VMS mogą zaoszczędzić wiele czasu i pieniędzy, analizując dane z miejskich ulic. Kamery Axis z wbudowanymi narzędziami do analiz LPR (Licence Plate Recognition) przekazują metadane – takie jak typ pojazdu, jego marka, kolor itp. – które następnie są przechowywane w bazie danych systemu VMS. Zgromadzenie wszystkich typów danych w jednej bazie wyszukiwania umożliwia szybkie, łatwe i efektywne prowadzenie prac wyjaśniających.

Mnogość kryteriów wyszukiwania

Wiele kamer Axis umożliwia wykorzystanie w nich otwartej platformy aplikacji ACAP (AXIS Camera Application Platform). Pierwsza wersja wtyczki AXIS Optimizer koncentruje się na aplikacjach ACAP z zakresu rozpoznawania tablic rejestracyjnych (LPR). Umożliwia wyszukiwanie w systemie Milestone XProtect metadanych pojazdów pochodzących z oferowanej przez Axis aplikacji AXIS License Plate Verifier oraz z aplikacji ACAP LPR, udostępnianych przez Vaxtor i FF Group. Połączenie tych danych sprawnie, że użytkownik systemu XProtect może przeszukiwać materiał wizyjny na podstawie wielu kryteriów:

- typu pojazdu, jego marki, modelu, koloru i prędkości;
- numerów tablic rejestracyjnych i kraju pochodzenia;
- daty i godziny zarejestrowania materiału wizyjnego.

Praktyczne zastosowania tego rozwiązania obejmują:

- Egzekwowanie przepisów dotyczących prędkości, pasów ruchu i sygnalizacji świetlnej;
- Zarządzanie ruchem na drogach;
- Pobór opłat drogowych;
- Wyjaśnianie przestępstw i wykroczeń w ruchu drogowym;
- Dbanie o bezpieczeństwo parkingów.

Szybkie i dokładne wyniki

Przetwarzanie metadanych i zarządzanie nimi z wykorzystaniem kamer IP zasilanych przez Ethernet (PoE) obniża koszty w porównaniu z przetwarzaniem ich na serwerze. Ponadto każda aplikacja w ramach platformy ACAP oraz kamera Axis są zoptymalizowane pod kątem zapewnienia wysokiej jakości materiału wizyjnego i analizy obrazu. Gwarantują to takie funkcje, jak zoom optyczny, automatyczne ustawianie ostrości, OptimizedIR, elektroniczna stabilizacja obrazu czy sterowanie czasem otwarcia migawki. W zależności od zastosowanej aplikacji w ramach platformy ACAP można uzyskać współczynnik poprawnej detekcji przekraczający nawet 97% oraz współczynnik poprawnego rozpoznania osiągający 95%.

Więcej informacji na stronie:
www.axis.com/products/axis-optimizer-for-milestone-xprotect/

INTEOX Bosch: otwarta platforma dozoru wizyjnego

Bosch ogłosił prowadzenie INTEOX – nowej, w pełni otwartej platformy dozoru wizyjnego, stworzonej z myślą o modernizacji i rozwoju branży zabezpieczeń. Oferuje użytkownikom, integratorom systemów oraz deweloperom aplikacji nieograniczoną swobodę tworzenia innowacyjnych i spersonalizowanych rozwiązań.

Budowanie przyszłości branży zabezpieczeń

Chcąc w pełni wykorzystać możliwości, jakie niesie IoT, branża zabezpieczeń musi wdrożyć konieczne zmiany. Bosch prezentuje ogromny potencjał IoT na przykładzie otwartej platformy dozoru wizyjnego INTEOX. Łączy ona funkcje inteligentnej analizy obrazu Bosch (Intelligent Video Analytics, IVA) z wyjątkową wydajnością, powszechnie stosowanym otwartym systemem operacyjnym i możliwością bezpiecznego dodawania aplikacji. Obsługuje najnowsze technologie, m.in. rozwiązania analityczne bazujące na sieci neuronowej – kolejny etap w dziedzinach uczenia maszynowego i sztucznej inteligencji. Otwarte platformy są koncepcją, która sprawdziła się już w branży komputerów i telefonii mobilnej. Aplikacje zapewniają szybki dostęp do informacji, bezpośrednie połączenie i szybką komunikację, poprawiają wydajność pracy i ułatwiają wykonywanie codziennych zadań. INTEOX umożliwia deweloperom aplikacji i integratorom systemów zabezpieczeń korzystanie z wbudowanej inteligencji oraz tworzenie nieograniczonej liczby aplikacji opartych na powszechnie używanym języku programowania. Równocześnie integratorzy systemów mogą personalizować systemy, aby dostosować je do potrzeb klienta poprzez dodawanie aplikacji oraz instalowanie ich w kamerach INTEOX.

Platforma INTEOX stanowi bazę całkowicie nowej generacji stałopozycyjnych i obrotowych kamer serii MIC, AUTODOME, FLEXIDOME oraz DINION, wspieranych przez otwartą infrastrukturę IoT. Infrastruktura ta, rozwijana przez należącego do Bosch start-up Security and Safety Things GmbH, opiera się na czterech filarach:

- Otwarty system operacyjny bazujący na Android Open Source Project, z rozszerzonym poziomem bezpieczeństwa;
- Sklep z aplikacjami (App Store) z dostępem do ważnych informacji o aplikacjach, opcją przeglądania oferty aplikacji dostępnych publicznie oraz możliwości zakupu gotowych do użycia aplikacji dla wszystkich kamer INTEOX;

- Portal internetowy dla deweloperów aplikacji i projektantów, oferujący informacje oraz narzędzia do tworzenia i testowania aplikacji;
- Portal do zarządzania urządzeniami, zapewniający dostęp do aktualnych danych o statusie urządzeń i pozwalający w łatwy sposób zarządzać aplikacjami.

Platforma INTEOX stanie się motorem innowacji wykraczających poza dzisiejsze możliwości pojedynczych przedsiębiorstw. Wprowadzenie otwartej platformy dozoru wizyjnego przyspieszy przyszły wzrost całej branży zabezpieczeń – mówi Michael Seiter, Senior Vice President, odpowiedzialny za segment Video Systems & Solutions w Bosch Building Technologies. Pierwsze kamery bazujące na platformie INTEOX będą dostępne na rynku najprawdopodobniej od lipca 2020 r. Więcej informacji na: <https://youtu.be/mCmxJlUbb0Q>

<https://www.boschsecurity.com/x/en/solutions/video-systems/open-camera-platform/>



Nowy Country Manager w Genetec



W ciągu ostatnich kilku lat Genetec odniósł wiele sukcesów, stając się ekspertem od zintegrowanego systemów zabezpieczeń. Firma ma bogate portfolio produktów, jest gotowa na podjęcie nowego ekscytującego wy-

Genetec, globalny dostawca technologii zunifikowanych rozwiązań w zakresie zabezpieczeń, bezpieczeństwa publicznego i business intelligence, w marcu br. powołał nowego Country Managera na region Niemiec, Austrii i Szwajcarii (DACH) oraz Europy Środkowo-Wschodniej (ECE). Został nim Kay Ohse, ekspert ds. IT, telekomunikacji i audio-wideo. Będzie odpowiedzialny za kontynuację rozwoju Genetec w tym regionie.

zwania – powiedział Kay Ohse. – Moim celem jest rozszerzenie zespołu sprzedaży w krajach DACH i ECE. W ścisłej współpracy z naszymi klientami i partnerami handlowymi będziemy rozwijali oraz wdrażali innowacyjne i kompleksowe rozwiązania bezpieczeństwa w wielu sektorach gospodarki.

Kay Ohse przeszedł do firmy Genetec z Kramer Electronics, międzynarodowego producenta rozwiązań audio i wideo, gdzie zajmował stanowisko Country Managera i był odpowiedzialny za rozwój kanałów oraz sprzedaż hurtową w Niemczech. Wcześniej pracował jako wi-

ceprezes ds. sprzedaży w Oracle Germany oraz Deutsche Telekom w dziale produktów i innowacji. Doświadczenie zdobywał także jako Country Manager DACH i ECE w firmie Polycom.

Z przyjemnością witam Kaya Ohse w roli Country Managera. Ma on międzynarodowe doświadczenie w budowaniu i rozwoju zespołów sprzedażowych. Jestem przekonany, że odniesie sukces w realizacji naszych ambitnych celów w podległym mu regionie – powiedział Francesco Serra, wiceprezes ds. sprzedaży w Europie w firmie Genetec.

Więcej na: www.genetec.com



Nowe NVR-y z serii Wisenet L z przełącznikiem sieciowym PoE



Łatwa konfiguracja

Czas pracy instalatorów na miejscu instalacji skraca się dzięki zdalnej łączności z rejestratorami przy użyciu smartfona lub tabletu, bez potrzeby skomplikowanej konfiguracji sieci. Instalacja sprowadza się do połączenia urządzeń (P2P) i zeskanowania kodu QR produktów. Rejestratory można też szybko skonfigurować wg wymagań użytkowników za pomocą udoskonalonego kreatora instalacji Wisenet, a także zdalnie aktualizować. Wszystkimi funkcjami rejestratorów z serii Wisenet L można zarządzać za pomocą klawiatury USB.

Wysoka wydajność

Modele 4-, 8- i 16-kanalowe oferujące wydajność nagrywania 30, 50 i 100 Mb/s (odpowiednio) oraz kompresję H.265, H.264 i MJPEG (do wyboru) umożliwiają rejestrowanie jednocześnie dwóch strumieni: w jakości 5 Mpix i VGA. Minimalizuje to opóźnienia odtwarzania wizji, które mogą się pojawić podczas zdalnego podglądu obrazu przy niskiej przepustowości sieci.

Inteligentne wyszukiwanie

Użytkownicy mogą korzystać z funkcji inteligentnego wyszukiwania na podstawie metadanych z kamery. Zarejestrowany materiał wizyjny można szybko znaleźć, stosując kryteria inteligentne-

Hanwha Techwin wyposażyla swoje nowe, atrakcyjne cenowo rejestratory sieciowe Wisenet L z wbudowanym przełącznikiem sieciowym PoE w funkcje, które zwrócą uwagę instalatorów i integratorów poszukujących dla swoich projektów ekonomicznego systemu dozoru wizyjnego. Wbudowane porty PoE umożliwiają zasilanie dowolnej kamery sieciowej zgodnej z tym standardem, co oznacza minimalizację kosztów i czasu instalacji.

go wyszukiwania zdarzeń (przekroczenie wirtualnej linii, wejście/wyjście do/z obiektu i detekcja ruchu, a także data/godzina, dziennik zdarzeń i transakcje kasowe EPOS).

Nowe rejestratory sieciowe stanowią doskonałe połączenie z naszymi kamerami Wisenet L i atrakcyjną cenowo opcję dla ekonomicznych systemów dozoru wizyjnego. Zestaw ich funkcji znacznie wykracza poza to, czego można oczekiwać od podstawowego urządzenia. W połączeniu z łatwością obsługi uzyskujemy idealne rozwiązanie do większości małych i średnich systemów — mówi Uri Guterman, szef Działu Produktów i Marketingu Hanwha Techwin Europe. □

DOSTĘPNE MODELE

– WISENET LRN-410S: 4-kanalowy NVR PoE, nagrywanie 30 Mb/s, miejsce na 1 dysk SATA (maks. 6 TB).

– WISENET LRN-810S: 8-kanalowy NVR PoE, nagrywanie 50 Mb/s, miejsce na 1 dysk SATA (maks. 6 TB).

– WISENET LRN-1610S: 16-kanalowy NVR PoE, nagrywanie 100 Mb/s, miejsce na 2 dyski SATA (łącznie maks. 12 TB).

BRIVO świętuje 20 lat innowacji w kontroli dostępu



BRIVO to światowy lider w dziedzinie systemów kontroli dostępu w chmurze. Jego misją jest dostarczanie rozwiązań innowacyjnych i prostych w użytkowaniu, gwarantujących najwyższy poziom bezpieczeństwa w chmurze. Łączy ponad 20 lat doświadczenia z najnowszymi osiągnięciami techniki.



Wyniki badań przeprowadzonych wśród integratorów i użytkowników końcowych tradycyjnych systemów KD wykazały duże problemy z oprogramowaniem, szczególnie pod kątem bezpieczeństwa w sieci (cybersecurity). Lokalne serwery przechowujące kluczowe informacje, takie jak dane dostępowe, można w prosty sposób zhakować. Ponadto takie systemy są drogie w utrzymaniu

i mało elastyczne (nie można szybko reagować na zmiany). System kontroli dostępu BRIVO oferuje inną architekturę, działa w chmurze. Zarządzamy nim zdalnie poprzez Internet, dzięki czemu możemy szybko reagować na bieżącą sytuację, np. ograniczając dostęp wybranych osób na dany teren. Całość komunikacji jest zawsze szyfrowana i odbywa się z serwerem w chmu-

rze. W ten sposób dane są bezpiecznie przechowywane w profesjonalnym data center gwarantującym najwyższy poziom bezpieczeństwa.

BRIVO to więcej niż system KD, to platforma oferująca i łącząca w jednym systemie zdalną kontrolę dostępu, transmisję i przetwarzanie danych, dozór wizyjny, zarządzanie uprawnieniami, domofonami i windami. Ponadto pozwala na autoryzację użytkownika za pomocą urządzenia mobilnego. W efekcie nie trzeba wydawać każdemu pracownikowi karty zbliżeniowej czy wydawać kluczy. Wykorzystując technologię Bluetooth lub NFC, drzwi można odblokować, naciskając przycisk w aplikacji lub przykładając telefon do czytnika obok wejścia. Jest to praktyczne i ekonomiczne rozwiązanie optymalizujące koszty.

Postęp i nieustanny rozwój technologii sprawił, że dziś BRIVO może pochwalić się ponad 20 milionami użytkowników w 42 krajach. □

Więcej na www.linc.pl



NIE KUPUJ KAMERY – wybierz pełne rozwiązanie w modelu Security as a Service

HEALTH INDICATOR®

KOMPLEKSOWY PROCES IDENTYFIKACJI TEMPERATURY CIAŁA I OCHRONY PRACOWNIKÓW

PROCEDURY I REGULAMINY (ZGODNE Z RODO I KODEKSEM PRACY) • PROFESJONALNY SYSTEM POMIARU TEMPERATURY CIAŁA • PEŁNA OBSŁUGA SERWISOWA Z GWARANCJĄ CIĄGŁOŚCI DZIAŁANIA • SZKOLENIA DLA PRACOWNIKÓW OCHRONY I/LUB RECEPCJI • TELEFON ALARMOWY 24H • PEŁNA MOBILNOŚĆ ROZWIĄZANIA I MOŻLIWOŚĆ SZYBKIEJ RELOKACJI

TRUSTMAN
www.trustman.pl



DS-K1TA70MI-T

DS-KAB671-B



DS-DM0710BL



Wygodny, wydajny i wielofunkcyjny

MinMoe Terminal do pomiaru temperatury Seria A70

Wiemy, że efektywność i wydajność ma kluczowe znaczenie dla wszystkich firm – dlatego staramy się tak projektować nasze urządzenia, aby były jak najbardziej wielofunkcyjne. Ponieważ systemy do pomiaru temperatury są ściśle powiązane z kontrolą dostępu prezentujemy rozwiązanie dostarczające obu funkcji w jednym, kompaktowym urządzeniu.

Jeden system, wiele możliwości.

- Termograficzny pomiar temperatury
- Temperatura powierzchni skóry wyświetlana jest na ekranie
- Wykrywanie maseczki i zablokowanie możliwości wejścia w przypadku jej braku
- Wiele możliwości instalacji
- Funkcja interkomu
- Możliwość integracji z istniejącymi systemami kontroli dostępu



DS-K1TA70MI-T

MinMoe Terminal do rozpoznawania twarzy

- Zakres pomiaru temperatury: 30 – 45°C, dokładność: 0.1°C, zakres błędów: $\pm 0.5^\circ\text{C}$
- Odległość pomiaru: 0.5 - 1.8 m
- Pojemność: 6.000 twarzy, 6.000 kart MIFAR

DS-KAB671-B

Stojak podłogowy (opcjonalnie)

- Dedykowany dla DS-K1TA70MI-T
- Wymiary (szer. x wys. x gł.): 98.5 x 1342 x 225 mm



DS-DM0710BL

Stojak nabełkowy (opcjonalnie)

- Dedykowany dla DS-K1TA70MI-T
- Wymiary (szer. x wys. x gł.): 192 x 353 x 195 mm

Hikvision Poland
Żwirki i Wigury 16B
02-092 Warszawa
T 22 460 01 50
info.pl@hikvision.com