03 (57) / 2026

CZASOPISMO RYNKU SECURITY

a&S POLSKA

MOBILNE WIEŻE MONITORINGU

Mobilny monitoring przestaje być wyłącznie kosztem ochrony, coraz częściej jest narzędziem wspierającym efektywność operacyjną. Mobilne wieże stają się kluczowym elementem nowoczesnych systemów ochrony.

NOWE ZADANIA OPERATORA

Norma PN-EN 62676 *Systemy dozoru wizyjnego* na nowo definiuje zadania operatora systemów telewizji dozorowej oraz wymagania dotyczące jakości obrazu w nowoczesnych systemach monitoringu.

SMART CITY DOJRZAŁO

Współczesne miasta redefiniują podejście do zarządzania przestrzenią publiczną. Coraz większą rolę odgrywają w nich zaawansowane systemy monitoringu wizyjnego wspierające bezpieczeństwo i organizację ruchu.

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

SALTO WECOSYSTEM

Nowy wymiar inteligentnego i bezpiecznego dostępu

Salto tworzy przyszłość cyfrowej transformacji w zarządzaniu dostępem i tożsamością, łącząc innowacyjne technologie z nowoczesnym, inteligentnym i bezpiecznym podejściem do ochrony ludzi oraz całych przestrzeni wszelkiego rodzaju obiektów.

Nasze rozwiązania w zakresie kontroli dostępu obejmują Kontrolę Dostępu, Rozpoznawanie Twarzy, Wideodomofony, Zarządzanie Tożsamością oraz Efektywność i Kontrolę Energii — zapewniają intuicyjne, bezpieczne i niezawodne działanie w różnych branżach, w stale zmieniającym się świecie.

ZAPRASZAMY DO NASZEGO BIURA ORAZ XSPERIENCE CENTRE W WARSZAWIE

salto
INSPIRED ACCESS

www. saltosystems.pl

Bezpieczne miasto zaczyna się od odporności

Jeszcze kilkanaście lat temu wizje inteligentnych miast opierały się głównie na technologii. Smart city miało być przestrzenią pełną ekranów, sensorów, autonomicznych pojazdów i aplikacji rozwiązujących problemy mieszkańców. Dziś podejście do projektowania miast wyraźnie się zmieniło. Kluczowe stały się odporność, bezpieczeństwo i jakość życia. Technologia nie zniknęła – przeciwnie, dojrzała i stała się narzędziem wspierającym funkcjonowanie miasta, a nie jego celem samym w sobie.

W raporcie *Smart city nie umarło. Dojrzało* (str. 14) pokazujemy, jak zmienia się sposób myślenia o nowoczesnych aglomeracjach. Jeszcze niedawno wiele zagrożeń uznawano za mało prawdopodobne scenariusze kryzysowe. Dziś stają się elementem codziennego zarządzania operacyjnego. Dotyczy to również monitoringu miejskiego, który przestaje być wyłącznie narzędziem rejestracji zdarzeń. Współczesne systemy dozoru stają się integralną częścią zarządzania bezpieczeństwem, ruchem i przestrzenią publiczną.

Dynamiczne zmiany zachodzą również w obszarze sztucznej inteligencji. W materiale *Inteligentne bezpieczeństwo w erze smart city – analiza rynku do 2030 roku* (str. 22) analizujemy, jak Europa przyspiesza wdrażanie systemów dozoru opartych na AI. Sztuczna inteligencja coraz częściej nie tylko wspiera operatorów, ale także staje się fundamentem nowoczesnych systemów bezpieczeństwa publicznego i ochrony infrastruktury krytycznej.

Nowoczesne miasta i przedsiębiorstwa coraz częściej sięgają także po rozwiązania mobilne. W artykule *Mobilny monitoring wizyjny: od kosztu bezpieczeństwa do narzędzia efektywności biznesowej* (str. 32) pokazujemy, dlaczego mobilne wieże monitoringu stają się ważnym elementem ochrony placów budowy, centrów logistycznych czy wydarzeń masowych. Mobilny monitoring przestaje być wyłącznie kosztem ochrony, coraz częściej pełni funkcję narzędzia wspierającego efektywność operacyjną i ciągłość działania.

W dziale *Głos branży – bezpieczne miasta* (str. 38) eksperci i praktycy dzielą się doświadczeniami dotyczącymi bezpieczeństwa współczesnych aglomeracji. Ich perspektywa pokazuje, że skuteczne zarządzanie bezpieczeństwem wymaga dziś integracji technologii, procedur i kompetencji ludzi.

Szczególną uwagę poświęcamy również kamerom nasobnym. W materiałach dotyczących ich wykorzystania przez policję, straż miejską oraz branżę ochrony (str. 42 i 46) analizujemy zarówno korzyści operacyjne, jak i rosnące wyzwania prawne związane z ochroną prywatności i przetwarzaniem danych.

Temat standardów rozwijamy w artykule poświęconym normie PN-EN 62676 (str. 48), gdzie pokazujemy nowe podejście do definiowania zadań operatora systemów dozoru wizyjnego oraz jakości obrazu wymaganej w nowoczesnych systemach monitoringu.

Na zakończenie polecamy relacje z naszych wydarzeń branżowych: konferencji *Infrastruktura krytyczna, energetyka i OZE* oraz jubileuszowej 10. edycji Security BootCamp. Choć różnią się formułą i zakresem tematycznym, oba wydarzenia na stałe wpisały się w kalendarz branży security i stanowią ważną przestrzeń wymiany wiedzy oraz doświadczeń. •

Redakcja

A&S POLSKA WYDANIE ONLINE: aspolska.pl

CZASOPISMO RYNKU SECURITY

a&S POLSKA

03 (57) / 2026

Spis treści

PRODUKTY NUMERU

BEZPIECZNE MIASTO

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. Złoczowska 25
03-972 Warszawa
info@aspolska.pl
www.aspolska.pl

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamakis
Adela Prochyra

DZIAŁ REKLAMY
Iwona Krawiec

DZIAŁ PROJEKTÓW SPECJALNYCH
Jolanta A. Kucharska
Aleksandra Czapska

CENTRUM KOMPETENCJI
Jacek Grzechowiak

KOREKTA
Jolanta Kucharska

PROJEKT GRAFICZNY I SKŁAD
Marta Kołodziejak

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

BCS

WIEŻA NA STRAŻY, TY NA PLAŻY

MOBILNY MONITORING TAM, GDZIE GO POTRZEBUJESZ

Błyskawiczne zabezpieczenie budów, parkingów i eventów. Dowolna konfiguracja: wybierz kamery, mikrofon, głośnik oraz czujniki, których aktualnie potrzebujesz.

Odkryj także Mini Tower – autonomiczny słupek alarmowy z zasilaniem solarnym oraz syreną 105 dB

Bądź na bieżąco z podglądem Live w Twoim telefonie dzięki technologii chmury

BCS-MCAM01

BCS-MCAM02

POLSKA MARKA BCS

>> Więcej przeczytasz na stronie 10

CZASOPISMO RYNKU SECURITY

a&S POLSKA

03 (57) / 2026

Spis treści

RYNEK SECURITY

CYBERBEZPIECZEŃSTWO

SERWIS INFORMACYJNY

Elara™ Seria R

TELEDYNE FLIR

System radarowy, oferujący zasięg wykrywania do 400 m i bardzo szerokie poziome pole widzenia 90°, umożliwiające monitorowanie dużych obszarów.

Skuteczne wykrywanie w trudnych warunkach

- Deszcz
- Mgła
- Śnieg
- Dym
- Niski kontrast termiczny

OFICJALNY DYSTRYBUTOR:
Linc Polska Sp. z o.o.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00
e-mail: info@linc.eu

www.linc.eu

WIĘCEJ O NAS:

Linc
Trusted Solutions

Z głębokim smutkiem przyjęliśmy wiadomość
o śmierci naszego Kolegi i Przyjaciela

Tomasza Migdała

(1975–2026)

Tomek był cenionym menedżerem i ekspertem branży systemów bezpieczeństwa oraz nowych technologii. Przez ponad dwadzieścia pięć lat aktywnie uczestniczył w budowaniu i rozwoju rynku nowoczesnych technologii bezpieczeństwa w Polsce.

Swoją drogę zawodową, po ukończeniu Szkoły Głównej Handlowej w Warszawie, rozpoczął w firmie SANTEC Industrial Video. Następnie w latach 2005–2012 związany był z firmą SPS Trading – pełnił tam funkcje Sales Managera działu systemów bezpieczeństwa oraz Sales Directora Distribution and Projects. Później objął stanowisko National Sales Managera w firmie Videor. Od 2013 roku współtworzył Hikvision Europe oraz Hikvision Poland – najpierw jako Country Sales Manager w Polsce, następnie General Manager, by ostatecznie pełnić funkcję Strategic Development & Marketing Directora.

Tomek był człowiekiem niezwykle zaangażowanym, życzliwym i otwartym na ludzi. Ceniliśmy Go za profesjonalizm, spokój, umiejętność budowania relacji oraz gotowość do dzielenia się wiedzą i doświadczeniem. Pozostawił po sobie nie tylko imponujący dorobek zawodowy, ale przede wszystkim pamięć dobrego Człowieka, Kolegi i Lidera.

Współpracował z naszą redakcją od samego początku. Wspierał nas przez wiele lat, dzięki czemu udało nam się osiągnąć pozycję lidera na rynku security. Miał też ogromny wkład w inicjatywę powołania konferencji Warsaw Security Summit. Zawsze mogliśmy liczyć na Jego wiedzę i doświadczenie, którymi chętnie dzielił się z naszymi Czytelnikami i uczestnikami organizowanych przez nas wydarzeń.

Był ekspertem i wartościowym rozmówcą, a także życzliwym partnerem w pracy, otwartym na dyskusję, gotowym do pomocy i zawsze znajdującym czas na rozmowę – nawet w najbardziej wymagających momentach. Jego komentarze i analizy cechowały się rzetelnością, spokojem oraz wyjątkową umiejętnością tłumaczenia złożonych zagadnień w sposób prosty i zrozumiały. Dzięki swojej kulturze osobistej, empatii i autentycznemu zaangażowaniu zyskał sympatię Czytelników i szacunek całej branży zabezpieczeń. Dla wielu był nie tylko cenionym współpracownikiem, ale także inspiracją i po prostu dobrym człowiekiem, którego będzie nam bardzo brakować.

Tomku, pozostaniesz w naszej pamięci na zawsze...

Redakcja a&s Polska

Tomasz, Tomek, Tomuś – kto go nie znał ręka do góry? Nie widzę? Tak myślałem.

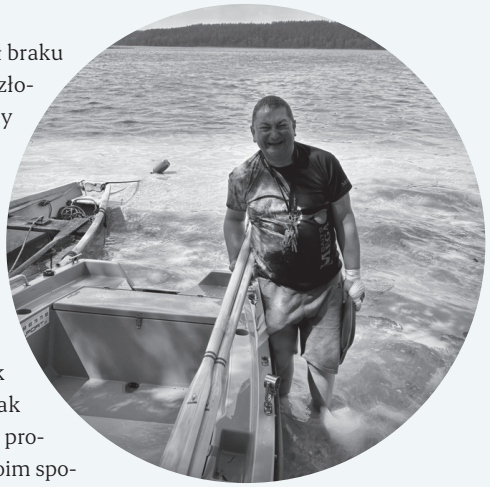
Profesjonalista, dla wielu Mentor i prawdziwy przyjaciel. Pasjonat! To słowo najlepiej w moim odczuciu oddaje jego charakter. Tomka poznałem biznesowo prawie 25 lat temu, to był inny rynek i zupełnie inne realia – o ludziach jego pokroju mówi się dzisiaj żartobliwie „Stare Wojsko". W czasach, kiedy nie było jeszcze mediów społecznościowych, biznes robiło się w zasadzie tylko poprzez relacje – Tomek był w pierwszej lidze, potrafił budować relacje jak mało kto, do tego wrodzony kunszt i obycie, miał w sobie coś takiego, co nakazywało wierzyć, że to, co mówi, po prostu będzie zrobione.

Tomek karierę w branży security rozpoczął w drugiej połowie lat dziewięćdziesiątych, gdzie w grupie wizjonerów i podobnych jemu profesjonalistów budował sprzedaż opartą na twardych zasadach i wartościach. Był, jest i będzie prawdziwym ojcem sukcesu marek Aper oraz Hikvision – w zasadzie każda kamera HIK-a, która wisi gdzieś w Polsce (i nie tylko), ma początek w determinacji Tomka w dążeniu do założonego celu.

A jaki był Tomek w pracy i życiu codziennym? Cierpliwy i analityczny. Jego bliscy przyjaciele wspominają, że Tomek nigdy nie podejmował decyzji „na pniu", zawsze dogłębnie analizował sprawy i szukał najlepszej drogi, potrafił słuchać innych i przyjmować rzeczowe argumenty – wypadkową jego działań była zawsze strategiczna analiza i konsultacja, miał nieprawdopodobny zmysł, który w połączeniu z pracowitością i pewnego rodzaju pozytywnym uporem pozwalał mu osiągać spektakularne sukcesy.

Tomek był mistrzem w budowaniu skutecznych zespołów zadaniowych, dlatego tak doskonale realizował i prowadził strategiczne projekty, banki, stadiony, fabryki – im większe, tym lepsze. Dla Tomka nie było rzeczy niemożliwych, a proces sprzedażowy jak nikt inny rozumiał od początku do końca (właściwie do nieskończoności, ponieważ relacje z Tomkiem zawierało się niejako na zawsze).

Tomek miał silne poczucie wartości własnych doświadczeń, potrafił słuchać ludzi, jednak rzeczowa obrona własnego zdania popartego wieloletnią praktyką była dla niego niezmiernie ważna. Nigdy jednak w konstruktywnej wymianie argumentów



nie obraził lub nie okazał braku szacunku do drugiego człowieka. Osobiście nigdy nie poznałem człowieka, który miałby z Tomkiem „na bakier", wręcz przeciwnie wszyscy darzyli go ogromną sympatią i zaufaniem. Myślę, że wynikało to z faktu, że raz dane słowo Tomek przekładał w czyny – jak dziś pamiętam trudności projektowe, które Tomek swoim spokojem i profesjonalnym podejściem odsyłał na drugi plan, bo problemy były od tego, żeby je dla Klienta skutecznie rozwiązywać, a nie zamiatać pod dywan!

Pracując z Tomkiem, miało się wyjątkowe wrażenie robienia czegoś wyjątkowego, czegoś dobrego dla branży i rynku – a jak mawiają jego przyjaciele, sprzedaż nie była nigdy celem samym w sobie. Tomek uwielbiał pracować – jako pasjonat swojej profesji łączył pracę z pasją życiową, jaką było wędkarstwo. Poprzez oddawanie się jej pozwalał głowie układać plany i z ryb zawsze wracał z gotowymi rozwiązaniami – to była jego wyjątkowa przestrzeń, której, podobnie jak pracy, potrafił się oddawać bez reszty. Kochał przyrodę i naturę – oddawał jej istotną część swojego życia. Potrafił cieszyć się z tego, że nad ranem mógł boso pochodzić po trawie. Gdy robiłem mu to ostatnie zdjęcie na wodzie, mówił mi, że tak wygląda szczęście.

Tomek wspaniale bawił się słowem, a jego głęboki spokojny głos pozostanie z nami na długo. Wraz z jego odejściem odchodzi pewien specyficzny rodzaj atmosfery i swoistej przyjaźni – Tomek był dla nas łącznikiem, a dla młodszych koleżanek i kolegów w wielu kwestiach wzorem do naśladowania.

Tomuś, Drogi Przyjacielu! Dziękujemy Ci za wszystko, co wniosłeś do naszej codzienności – do zobaczenia kiedyś na niebieskiej autostradzie.

Rafał Łupkowski i przyjaciele z Płaskiej

Z ogromnym smutkiem i niedowierzaniem przyjęliśmy wiadomość o śmierci Tomka.

Tomek był założycielem i wieloletnim liderem polskiego oddziału Hikvision. To właśnie dzięki jego wizji, zaangażowaniu i determinacji firma mogła rozwijać się w Polsce od samego początku. Przez wiele lat był nie tylko General Managerem, ale przede wszystkim człowiekiem, który potrafił budować relacje, inspirować ludzi i tworzyć wyjątkową atmosferę wokół siebie.

W pamięci wielu z nas pozostanie osobą niezwykle ciepłą, otwartą i serdeczną. Tomek miał rzadki dar sprawiania, że ludzie czuli się mile widziani i ważni. Był gospodarzem z sercem, liderem bliskim ludziom i człowiekiem, z którym po prostu dobrze było być, zarówno w pracy, jak i poza nią. Dla wielu osób był nie tylko przełożonym czy partnerem biznesowym, ale także mentorem i przyjacielem. Pozostawił po sobie ogromny ślad w firmie, w branży i przede wszystkim w sercach ludzi, których spotkał na swojej drodze.

Rodzinie, bliskim oraz wszystkim, którzy mieli zaszczyt znać i współpracować z Tomkiem, składamy najszczersze wyrazy współczucia.

Tomku – dziękujemy za wszystko. Będziemy o Tobie pamiętać.

Koleżanki i koledzy z Hikvision Poland

Prezentujemy najnowsze urządzenia z oferty firm

BCS, HIKVISION, SYNOLOGY, TP-LINK, VCS

BCS

Domofony BCS POINT

Współczesne systemy kontroli dostępu coraz częściej łączą funkcjonalność, prostotę obsługi oraz integrację z systemem CCTV. Wymagania te spełnia linia BCS POINT, której przykładem jest zestaw wideodomofonowy z jednoprzyciskowym panelem BCS-P-PAN1000G/1101G oraz monitorem BCS-P-MON7100B/W. Rozwiązanie jest przeznaczone do pojedynczych lokali, w których kluczowe znaczenie mają niezawodna identyfikacja oraz intuicyjna komunikacja.

Panel zewnętrzny BCS-P-PAN1000G/PAN1101G stanowi minimalistyczny, ale w pełni funkcjonalny punkt wejścia. Jednoprzyciskowa obsługa eliminuje błędy i skraca czas wywołania. Kamera 2 Mpix z podświetleniem podczerwonym zapewnia obraz w jakości Full HD niezależnie od warunków oświetleniowych, a czytnik MIFARE zapewnia szybki i wygodny dostęp bez użycia fizycznych kluczy.

Urządzenie pracuje w technologii IP oraz wspiera kodeki H.264 i H.265, co pozwala na efektywną transmisję obrazu przy niskim obciążeniu sieci. Obudowa o klasie szczelności IP65 oraz szeroki zakres temperatury pracy gwarantują stabilność działania w warunkach zewnętrznych. System można rozszerzyć o ramkę z daszkiem, poprawiającą czytelność obrazu w silnym świetle.

Uzupełnieniem zestawu jest monitor BCS-P-MON7100B/W – 7-calowy, pojemnościowy ekran dotykowy pełniący funkcję centrum komunikacji i nadzoru. Umożliwia podgląd kamer IP, obsługę wejść alarmowych oraz integrację z aplikacją mobilną BCS Point, zapewniając zdalny dostęp do systemu.

Całość tworzy spójny ekosystem odpowiadający na potrzeby rynku w zakresie bezpieczeństwa, wygody oraz elastyczności instalacji. •

Więcej na: www.bcs.pl

HIKVISION

DS-2CD2387G3P-LIS2UY/SL(180°)(O-STD)

Hikvision DS-2CD2387G3P-LIS2UY/SL(180°)(O-STD) to nowoczesna kamera panoramiczna nowej generacji, zaprojektowana z myślą o monitoringu dużych przestrzeni bez typowych zniekształceń obrazu charakterystycznych dla klasycznych kamer panoramicznych. W standardowych rozwiązaniach obiekty znajdujące się przy krawędziach kadru często są rozciągnięte i nienaturalnie zdeformowane, co utrudnia identyfikację osób oraz analizę zdarzeń. Model Hikvision eliminuje ten problem dzięki zaawansowanej technologii łączenia obrazu, zachowując naturalne proporcje obiektów w całej scenie – nawet przy niewielkiej odległości od obserwowanego obszaru.

Jednym z kluczowych atutów urządzenia jest panoramiczny format 20:9, oferujący niemal dwukrotnie większe pole widzenia niż tradycyjne rozwiązania 32:9, przy jednoczesnym zachowaniu bardziej naturalnej perspektywy. Dzięki temu operator otrzymuje szeroki obraz bez efektu „rozciągania" osób czy przedmiotów.

Kamera oferuje rozdzielczość 8 Mpix i wykorzystuje technologię ColorVu 3.0, zapewniając kolorowy obraz przez całą dobę, nawet przy bardzo słabym oświetleniu. Funkcja Smart Hybrid Light inteligentnie przełącza podświetlenie IR oraz światło białe, natomiast AcuSense 3.0 umożliwia skuteczne rozróżnianie ludzi i pojazdów, ograniczając liczbę fałszywych alarmów.

Dodatkowe funkcje, takie jak aktywne odstraszanie światłem i dźwiękiem, wbudowane mikrofony, dwukierunkowe audio oraz odporna obudowa o klasie szczelności IP67, sprawiają, że kamera doskonale sprawdza się w obiektach logistycznych, przemysłowych, handlowych oraz przestrzeniach publicznych. •

Więcej na: www.hikvision.com/pl/

RACS 5

roger
ASSA ABLOY

Nowoczesna transformacja bez rewolucji

Nowy system, ta sama instalacja.
Wykorzystaj istniejącą infrastrukturę i zyskaj nowe możliwości.

Maksymalne bezpieczeństwo. Minimalny wysiłek.
Protokół OSDP, szyfrowana komunikacja, Grade 4 – najwyższy poziom w standardzie.

Nowoczesność w praktyce: efektywność, komfort, elastyczność.
Wydajna baza SQL, bezpieczna identyfikacja mobilna i wielostanowiskowa architektura.

Jeden system. Pełna kontrola.
Zarządzaj dostępem, monitoruj i wizualizuj zintegrowane systemy bezpieczeństwa – wszystko z jednego miejsca.

Technologia, która myśli jak Ty.
Nowoczesny interfejs, intuicyjna obsługa, pełna kontrola.

Zainwestuj w przyszłość – dziś.
RACS 5 to długoterminowe wsparcie i rozwój.

Experience a safer
and more open world

SYNOLOGY

Synology BC800Z – inteligentna kamera dla bezpiecznych miast

Bezpieczeństwo miast coraz rzadziej oznacza jedynie zapis obrazu. Dziś liczą się szybka analiza, automatyczna reakcja oraz integracja monitoringu z innymi systemami. Synology BC800Z doskonale wpisuje się w ten kierunek – sprawdzi się przy wjazdach, na parkingach, terenach przemysłowych oraz w przestrzeniach publicznych.

Kamera wykorzystuje funkcje AI, w tym rozpoznawanie tablic rejestracyjnych. Po podłączeniu do serwera Synology z Surveillance Station technologia ta może służyć nie tylko identyfikacji pojazdów, ale również automatyzacji dostępu. Rozpoznana tablica może uruchomić otwarcie bramy dla uprawnionego pojazdu – bez pilotów i bez angażowania ochrony.

Synology BC800Z potrafi również wykrywać dym na podstawie analizy obrazu. To szczególnie istotne na rozległych terenach, placach składowych oraz wszędzie tam, gdzie montaż klasycznych czujników dymu jest utrudniony. Wczesne powiadomienie może skrócić czas reakcji i ograniczyć skutki pożaru.

Dzięki API dostępnemu w Surveillance Station system może komunikować się z rozwiązaniami zewnętrznymi i stać się częścią większego ekosystemu bezpieczeństwa. Z kolei obsługa ONVIF ułatwia współpracę z systemami innych producentów, również podczas modernizacji istniejących instalacji.

Dodatkowym argumentem są certyfikaty NDAA/TAA. W Polsce nie zawsze mają one kluczowe znaczenie, jednak w obiektach o znaczeniu krytycznym pomagają wybrać zaufane rozwiązanie. BC800Z pokazuje, że monitoring może nie tylko nagrywać obraz, lecz także realnie wspierać bezpieczeństwo miasta. •

Więcej na: www.synology.com/pl

TP-LINK

Porty do 100G, zaawansowany routing L3 i łączenie w stos: TP-Link prezentuje przełączniki Omada Campus

Cyfrowa transformacja i lawinowy przyrost przesyłanych danych stawiają przed firmami nowe wyzwania infrastrukturalne. Odpowiedzią na te potrzeby jest najnowsza seria przełączników Omada Campus od TP-Link. Zostały zaprojektowane z myślą o budowie wysoce wydajnych, skalowalnych i bezpiecznych sieci korporacyjnych klasy Enterprise, które sprawdzą się w kampusach, hotelach oraz dużych biurowcach.

Nowa linia produktowa dzieli się na dwa kluczowe segmenty. Pierwszym z nich jest seria S7500 – zarządzalne przełączniki rdzeniowe i agregacyjne, stanowiące szkielet całej infrastruktury. Wyposażone wyłącznie w szybkie porty światłowodowe 10G, 25G oraz imponujące 100G, gwarantują błyskawiczną wymianę danych między serwerowniami. Obsługują zaawansowany routing L3, fizyczne łączenie w stos oraz niezawodną technologię M-LAG, minimalizując ryzyko przestojów.

Drugim filarem jest seria S6500, czyli wielogigabitowe przełączniki warstwy dostępowej. Służą one do bezpośredniego podłączania urządzeń końcowych, takich jak punkty dostępowe czy kamery IP. Wybrane modele oferują technologię PoE++ o mocy do 90 W na port, co ułatwia zasilanie nowoczesnego sprzętu IT.

Cała rodzina Omada Campus wyróżnia się wielopoziomowym bezpieczeństwem (m.in. Secure Boot oraz 802.1X) oraz możliwością centralnego zarządzania w chmurze za pośrednictwem platformy Omada. Produkty objęte są 5-letnią gwarancją producenta. •

Więcej na: www.tp-link.com/pl/

VCS

iTower™ by VCS – monitoring zasilany niezależnością

Jeśli potrzebujesz czasowej ochrony w miejscu pozbawionym infrastruktury energetycznej i sieciowej, interesującym rozwiązaniem są mobilne wieże do monitoringu wizyjnego. Warto jednak pamiętać, że nie każda wieża oferuje takie same możliwości.

Jeśli oczekujesz rozwiązania łatwego w transporcie i szybkim rozkładaniu, stabilnego oraz umożliwiającego indywidualną konfigurację wyposażenia, właściwym wyborem będzie iTower™ by VCS.

Kluczowe atuty wieży iTower™ by VCS

Monitoring tam, gdzie kończy się infrastruktura. Wieża została wyposażona w lekkie, innowacyjne i odporne na uszkodzenia giętkie panele słoneczne (3 × 240 W), zamontowane pod optymalnym kątem padania promieni słonecznych, co zwiększa ich wydajność.

Dodatkowo iTower™ może być zasilana akumulatorowo (do 4 baterii) lub za pomocą ogniwa paliwowego na metanol, co zapewnia wysoką autonomię działania.

Inteligentna konstrukcja, nieograniczone możliwości. Kompaktowa i lekka konstrukcja oraz składany maszt ułatwiają transport, a ergonomiczny system podwójnych drzwi i stabilna budowa masztu umożliwiają instalację praktycznie dowolnych urządzeń, m.in. kamer, lamp, radarów, rejestratorów czy systemów zasilania. Dodatkowym atutem jest zamknięta konstrukcja, chroniąca wnętrze przed zabrudzeniami oraz wpływem warunków atmosferycznych.

Bezpieczne i szybkie posadowienie. Stabilna konstrukcja wsparta podporami pozwala na szybkie i bezpieczne ustawienie wieży w terenie.

Wieża iTower™ by VCS zdobyła Złoty Medal Targów Securex 2026. •

Więcej na: www.vcs.pl

Linc
Trusted Solutions

iTOWER®

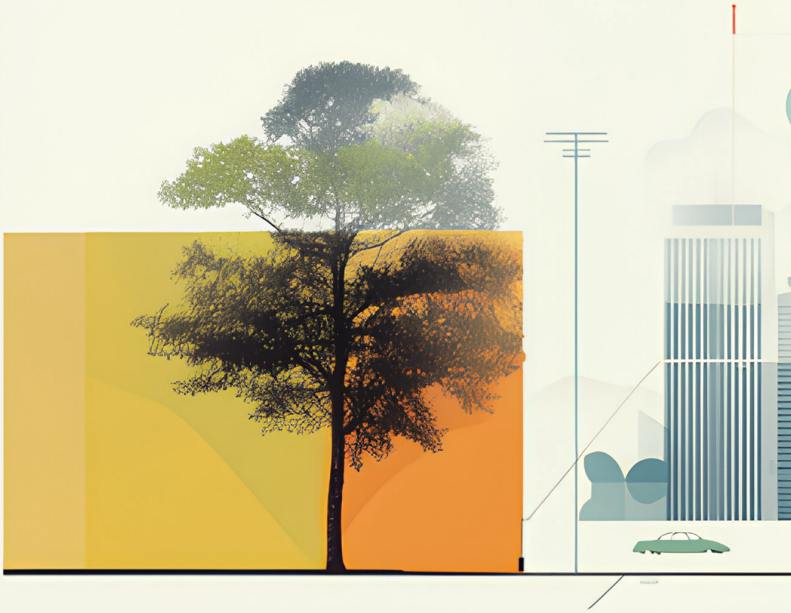
TAM GDZIE STANDARDOWE ZABEZPIECZENIA SIĘ
NIE SPRAWDZAJĄ TAM JESTEŚMY MY.

Mobilne rozwiązania do ochrony

- WŁASNE ZASILANIE
- MULTISPEKTRALNOŚĆ
- NIEZALEŻNOŚĆ
- OSZCZĘDNOŚĆ
- WYTRZYMAŁOŚĆ
- BEZPIECZEŃSTWO DOSTĘPU

www.linc.eu

Smart city nie umarło. Dojrzało



Kilkanaście lat temu miasta przyszłości wyglądały w prezentacjach niemal identycznie. Szklane przystanki z ekranami dotykowymi, autonomiczne autobusy, tysiące sensorów, inteligentne latarnie, aplikacje do wszystkiego i wszechobecna technologia, która miała rozwiązać większość problemów współczesnych aglomeracji. Dziś miasta projektuje się już nie wokół technologii, ale wokół odporności. Konkurują one między sobą jakością życia mieszkańców. Czy to znaczy, że technologii już nie ma? Wręcz przeciwnie.

Smart city stało się jednym z najmodniejszych pojęć w urbanistyce, administracji i technologii. Było obietnicą miasta bardziej efektywnego, nowoczesnego i lepiej zarządzanego. Okazało się jednak, że przyszłość nie należy do tych najbardziej naszpikowanych technologią. Tylko do tych, w których ludzie po prostu chcą żyć.

Dziś coraz rzadziej mówi się o samym smart city. Przynajmniej nie w sposób, w jaki robiono to jeszcze dekadę temu. To nie znaczy, że idea inteligentnego miasta zniknęła. Wręcz przeciwnie, ona dojrzała. Zmieniły się priorytety. Technologia przestała być celem samym w sobie. Stała się narzędziem. A mieszkańcy coraz częściej zaczęli zadawać bardzo proste pytania: czy w tym mieście żyje się dobrze? Czy miasto jest bezpieczne? Czy jest odporne na kryzysy? Czy daje poczucie komfortu i przewidywalności? Bo szybko okazało się, że miasto pełne technologii nie zawsze musi być miastem przyjaznym.

Smart, czyli jakie?

W wielu miejscach na świecie pierwsza fala projektów smart city zaczęła budzić również krytykę. Zarzucano jej oderwanie od realnych potrzeb mieszkańców, nadmierną fascynację technologią i tworzenie rozwiązań, które dobrze wyglądały w materiałach promocyjnych, ale niekoniecznie poprawiały codzienne funkcjonowanie miasta. Inteligentne ławki z ładowarkami USB czy interaktywne kioski informacyjne stały się symbolem pewnej epoki – momentu, w którym miasta próbowały być smart, czasem zapominając, po co właściwie wdrażają technologię. Równolegle zmieniał się też sam świat.

Pandemia COVID-19 pokazała, jak ogromne znaczenie mają lokalność, dostępność usług i odporność infrastruktury miejskiej. Kryzysy energetyczne uświadomiły skalę zależności od stabilnych systemów zasilania. Zmiany klimatyczne zaczęły wymuszać nowe podejście do projektowania przestrzeni miejskich. Do tego doszły cyberzagrożenia, przeciążenie infrastruktury, problemy transportowe i rosnące poczucie niepewności.

Przyszłość bezpieczeństwa będzie rozgrywać się przede wszystkim w miastach. Do 2050 roku będzie w nich mieszkało około 68% światowej populacji. Dziś jest to ok. 56%

Źródło: ONZ

W efekcie współczesne miasta coraz częściej odchodzą od wizji futurystycznej metropolii zarządzanej wyłącznie przez dane i algorytmy. Znacznie ważniejsze stają się dziś pojęcia takie jak *urban resilience, human-centric city, 15-minute city* czy *wellbeing city*. W centrum uwagi znalazł się człowiek – jego codzienne doświadczenia, bezpieczeństwo, zdrowie psychiczne, komfort życia i poczucie wpływu na przestrzeń wokół siebie.

To właśnie dlatego najlepsze współczesne miasta coraz rzadziej epatują technologią. Najbardziej zaawansowane rozwiązania są często niemal niewidoczne dla mieszkańców. Dobrze działający monitoring miejski nie zwraca na siebie uwagi, ale zwiększa poczucie bezpieczeństwa. Inteligentne systemy zarządzania ruchem nie muszą wyglądać futurystycznie – mają po prostu ograniczać chaos i poprawiać płynność komunikacji. Nowoczesne osiedla mieszkaniowe coraz częściej projektowane są nie wokół technologicznych gadżetów ale wokół wygody codziennego życia, bezpieczeństwa i jakości wspólnych przestrzeni.

Zmieniło się również podejście do samego bezpieczeństwa. Jeszcze kilka lat temu systemy security były często traktowane jako osobna warstwa infrastruktury miasta, dodatek do urbanistyki i architektury. Dziś coraz częściej stają się integralnym elementem projektowania przestrzeni miejskiej. Monitoring miejski, zabezpieczenia antyterrorystyczne czy inteligentna analiza obrazu nie są już wyłącznie narzędziami reagowania na incydenty. Mają wspierać codzienne funkcjonowanie miasta, poprawiać jakość życia mieszkańców i budować odporność całych systemów miejskich.

Nowoczesne miasto nie jest więc dziś smart dlatego, że ma najwięcej sensorów. Jest inteligentne wtedy, gdy technologia działa w tle, dyskretnie wspierając mieszkańców, przewidując zagrożenia i pomagając miastu funkcjonować sprawnie nawet w czasach rosnącej niepewności.

Być może właśnie dlatego współczesne smart city coraz rzadziej przypomina futurystyczną wizję z dawnych prezentacji technologicznych. A coraz bardziej dobrze zaprojektowane miejsce do życia.

Nowe miasto: zielone, lokalne i odporne

Jednym z najmocniejszych trendów ostatnich lat stała się idea miasta 15-minutowego – modelu urbanistycznego zakładającego, że najważniejsze potrzeby mieszkańca powinny być dostępne w krótkim czasie od miejsca zamieszkania. Praca, szkoła, transport publiczny, sklepy, usługi, zieleń czy przestrzenie społeczne mają znajdować się „blisko", bez konieczności codziennego przemieszczania się przez całe miasto. To odpowiedź nie tylko na

problemy komunikacyjne i środowiskowe, ale również na zmieniający się styl życia mieszkańców.

Pandemia przyspieszyła proces lokalizacji codzienności – wiele osób zaczęło spędzać więcej czasu w swojej najbliższej okolicy i zwracać uwagę na jakość przestrzeni, która wcześniej była jedynie „miejscem do spania". W praktyce oznacza to zupełnie nowe podejście do projektowania miast i osiedli. Coraz większe znaczenie mają przestrzenie wspólne, lokalne usługi, tereny zielone, infrastruktura rowerowa, bezpieczeństwo pieszych i możliwość naturalnego budowania relacji społecznych.

Dobrze zaprojektowane miasto ma dziś nie tylko działać sprawnie, ale również zmniejszać poziom codziennego stresu mieszkańców. Nieprzypadkowo wiele współczesnych inwestycji mieszkaniowych zaczyna przypominać niewielkie, samowystarczalne mikro miasta. Deweloperzy projektują dziś nie tylko budynki, ale także całe doświadczenie życia: przestrzenie coworkingowe, strefy rekreacyjne, zielone dziedzińce, punkty usługowe czy systemy bezpieczeństwa zintegrowane z codziennym funkcjonowaniem mieszkańców.

Zielone miasta to już nie trend. To konieczność

Drugim wielkim kierunkiem zmian jest redefinicja relacji między miastem a środowiskiem naturalnym. Jeszcze kilka lat temu „zielone miasto" kojarzyło się głównie z ekologią i estetyką. Dziś coraz częściej mówi się o nim w kontekście bezpieczeństwa i odporności infrastruktury. Rosnąca temperatura, gwałtowne opady, problemy z retencją wody czy przeciążenie systemów energetycznych sprawiają, że miasta muszą projektować przestrzenie inaczej niż jeszcze dekadę temu. Zieleń przestaje być dodatkiem do architektury. Staje się elementem infrastruktury krytycznej miasta.

Przykładem mogą być tzw. miasta gąbki, rozwijane m.in. w Singapurze czy chińskich metropoliach, gdzie przestrzeń projektowana jest w taki sposób, by naturalnie zatrzymywać wodę i ograniczać skutki gwałtownych opadów. W Kopenhadze rozwój infrastruktury rowerowej i zielonych przestrzeni od lat stanowi element strategicznego planowania miasta, a nie wyłącznie polityki środowiskowej. Z kolei Paryż konsekwentnie ogranicza ruch samochodowy w centrum, odzyskując przestrzeń dla mieszkańców.

To samo podejście zaczyna być widoczne również w inwestycjach komercyjnych i mieszkaniowych. Zielone dachy, retencja wody, energooszczędność, lokalne źródła zasilania czy odporność budynków na zakłócenia energetyczne stają się coraz ważniejszym elementem projektowania nowoczesnych osiedli i obiektów użyteczności publicznej.

Od *smart* do *resilient*

Jednym z najważniejszych słów w dyskusji o współczesnych miastach staje się dziś

resilience, czyli odporność. To pojęcie znacznie szersze niż klasyczne bezpieczeństwo. Oznacza zdolność miasta do funkcjonowania mimo kryzysów, przeciążeń i nieprzewidywalnych zdarzeń. Jeszcze kilka lat temu odporność kojarzono głównie z katastrofami naturalnymi. Dziś lista zagrożeń jest znacznie dłuższa: cyberataki, blackouty, przeciążenie infrastruktury, sabotaż, ataki terrorystyczne, dezinformacja, kryzysy energetyczne czy zakłócenia łańcuchów dostaw. To właśnie dlatego nowoczesne miasta coraz częściej projektowane są nie wokół maksymalnej efektywności, ale wokół zdolności adaptacji. Systemy miejskie mają nie tylko działać szybko i wygodnie, ale również utrzymywać ciągłość działania w sytuacjach kryzysowych.

Zmienia się także sposób myślenia o bezpieczeństwie w przestrzeni publicznej. Dobrze zaprojektowane miasto ma być jednocześnie otwarte i bezpieczne. Coraz większą rolę odgrywa więc projektowanie *security by design*, niewidzialnych zabezpieczeń wpisanych w architekturę miasta. Dotyczy to zarówno monitoringu miejskiego, zabezpieczeń antyterrorystycznych, jak i systemów kontroli dostępu czy ochrony infrastruktury transportowej. W praktyce oznacza to, że bezpieczeństwo coraz rzadziej jest „dokładane" do miasta na końcu procesu inwestycyjnego. Staje się jednym z fundamentów współczesnego projektowania urbanistycznego.

I właśnie w tym miejscu zaczyna się nowy rozdział dla rynku security. Bo inteligentne miasto przyszłości nie będzie miastem pełnym technologii widocznej na każdym kroku. Będzie miastem, które potrafi działać spokojnie, przewidywalnie i bezpiecznie.

Monitoring przestał być tylko „okiem miasta"

Monitoring miejski jeszcze do niedawna kojarzył się głównie z rejestracją obrazu i późniejszym odtwarzaniem nagrań po incydencie. Dziś jego rola wygląda zupełnie inaczej. Kamery stają się elementem systemów zarządzania przestrzenią miejską, ruchem i bezpieczeństwem operacyjnym całego miasta. Rozwój analityki obrazu i sztucznej inteligencji sprawił, że współczesne systemy monitoringu coraz częściej potrafią analizować sytuację w czasie rzeczywistym. Nie chodzi już wyłącznie o obserwację. Systemy mają wykrywać nietypowe zachowania, identyfikować zagrożenia, wspierać zarządzanie tłumem czy poprawiać bezpieczeństwo w przestrzeniach publicznych.

W wielu miastach monitoring wykorzystywany jest dziś do:

- analizy natężenia ruchu,
- wykrywania niebezpiecznych sytuacji drogowych,
- ochrony transportu publicznego,
- zarządzania bezpieczeństwem podczas wydarzeń masowych,
- wykrywania pozostawionych przedmiotów,
- ochrony infrastruktury krytycznej,
- monitorowania stref o podwyższonym ryzyku.

Coraz większe znaczenie ma również bezpieczeństwo psychologiczne mieszkańców. Dobrze oświetlone i monitorowane przestrzenie publiczne wpływają na sposób korzystania z miasta – szczególnie wieczorem i w miejscach o dużym natężeniu ruchu. W wielu projektach urbanistycznych monitoring staje się więc elementem budowania poczucia komfortu, a nie wyłącznie narzędziem reagowania na zagrożenia.

Jednocześnie miasta coraz częściej próbują znaleźć równowagę między bezpieczeństwem a prywatnością mieszkańców. Dyskusja wokół wykorzystania AI w monitoringu czy analizy danych miejskich staje się jednym z najważniejszych tematów współczesnego smart city. Technologia ma zwiększać bezpieczeństwo, ale nie może prowadzić do poczucia kontroli. To właśnie dlatego najlepiej oceniane systemy security są dziś niemal niewidoczne dla mieszkańców. Mają działać skutecznie, ale dyskretnie wpisywać się w tkankę miasta.

Bezpieczna przestrzeń nie może wyglądać jak twierdza

Zmienia się również podejście do fizycznego zabezpieczania przestrzeni publicznych. Współczesne miasta coraz częściej muszą projektować przestrzenie odporne na zagrożenia związane z terroryzmem, agresją czy niekontrolowanym ruchem pojazdów. Jednocześnie mieszkańcy oczekują przestrzeni otwartych, estetycznych i przyjaznych. To jeden z największych paradoksów współczesnej urbanistyki: jak projektować bezpieczne miasta, które nie przypominają stref wysokiego ryzyka?

W odpowiedzi na to wyzwanie rozwija się koncepcja *security by design* – bezpieczeństwa wpisanego w architekturę miasta. Bariery zabezpieczające, słupki antyterrorystyczne czy systemy kontroli ruchu coraz częściej projektowane są w taki sposób, by stawały się naturalnym elementem przestrzeni miejskiej.

W Londynie czy Nowym Jorku zabezpieczenia antyterrorystyczne coraz częściej przybierają formę elementów małej architektury: donic, ławek, zieleni czy dekoracyjnych słupków. Miasto ma pozostać otwarte i przyjazne, nawet jeśli pod powierzchnią funkcjonuje rozbudowany system ochrony. To podejście coraz wyraźniej widać również w nowoczesnych inwestycjach komercyjnych i mieszkaniowych. Deweloperzy nie chcą już budować zamkniętych twierdz odcinających mieszkańców od otoczenia.

Znacznie większe znaczenie mają dziś:

- inteligentna kontrola dostępu,
- dyskretne systemy bezpieczeństwa,
- ochrona stref wspólnych,
- bezpieczeństwo parkingów i garaży,
- integracja security z architekturą budynku.

Mieszkańcy oczekują bezpieczeństwa, ale jednocześnie nie chcą żyć w przestrzeni przypominającej obiekt wojskowy.

Infrastruktura miejska stała się nowym celem

Współczesne miasta są dziś znacznie bardziej zależne od technologii niż jeszcze dekadę temu. Systemy energetyczne, transport publiczny, wodociągi, centra danych, inteligentne budynki czy infrastruktura komunikacyjna tworzą jeden połączony organizm. Problem polega na tym, że im bardziej połączone staje się miasto, tym bardziej rośnie jego podatność na zakłócenia. Dlatego bezpieczeństwo infrastruktury miejskiej coraz częściej staje się jednym z najważniejszych tematów dla samorządów i operatorów obiektów użyteczności publicznej.

Rosnące zagrożenia cybernetyczne, możliwość sabotażu infrastruktury, blackouty czy przeciążenia systemów sprawiają, że miasta muszą myśleć o security znacznie szerzej niż tylko w kontekście ochrony fizycznej.

Nowoczesne systemy bezpieczeństwa coraz częściej łączą:

- monitoring miejski,
- cyberbezpieczeństwo,
- analizę danych,
- automatykę budynkową,
- systemy komunikacji kryzysowej,
- zarządzanie incydentami,
- kontrolę dostępu,
- ochronę perymetryczną.

Granica między security a zarządzaniem operacyjnym miasta zaczyna się zacierać. To szczególnie widoczne w obiektach infrastruktury krytycznej i użyteczności publicznej – szpitalach, centrach transportowych, urzędach, obiektach sportowych czy dużych kompleksach mieszkaniowych. Tam bezpieczeństwo coraz częściej oznacza zdolność do utrzymania ciągłości działania nawet w sytuacjach kryzysowych.

INTELIGENTNE ROZWIĄZANIA MIEJSKIE MOGĄ:

- skrócić czas dojazdów o **15–20%**,
- skrócić czas reakcji służb ratunkowych o **20–35%**,
- ograniczyć przestępczość nawet o **30–40%** w wybranych obszarach,
- zmniejszyć liczbę ofiar śmiertelnych dzięki inteligentnemu zarządzaniu ruchem o **8–10%**.

Źródło: McKinsey

Security stało się elementem doświadczenia mieszkańca

Jeszcze niedawno rozwiązania security w budynkach mieszkalnych były traktowane głównie jako infrastruktura techniczna – domofon, kamera przy wejściu, szlaban na parkingu. Dziś bezpieczeństwo coraz częściej staje się integralnym elementem całego doświadczenia mieszkańca. Nowoczesne inwestycje projektowane są wokół komfortu codziennego funkcjonowania. Mieszkańcy oczekują, że przestrzeń będzie nie tylko estetyczna, ale również bezpieczna. Chcą mieć kontrolę nad dostępem do budynku, poczucie prywatności w częściach wspólnych i możliwość swobodnego korzystania z infrastruktury osiedla. W efekcie

security zaczyna działać w tle codziennego życia – dyskretnie, ale stale.

Osiedla muszą być bezpieczne, ale nie zamknięte

Zmienia się również filozofia samego projektowania przestrzeni mieszkaniowych. Jeszcze przez wiele lat symbolem bezpieczeństwa były osiedla zamknięte – odcięte od miasta płotami, bramami i systemami kontroli dostępu. Dziś coraz więcej urbanistów i deweloperów odchodzi od tego modelu. Nowoczesne inwestycje mają być otwarte, zielone i społecznie aktywne, ale jednocześnie zapewniać mieszkańcom poczucie bezpieczeństwa. To ogromne wyzwanie projektowe. Przestrzeń musi zachęcać do życia społecznego i korzystania z części wspólnych, a jednocześnie ograniczać ryzyko incydentów, wandalizmu czy niekontrolowanego dostępu.

Coraz większą rolę odgrywa więc projektowanie „bezpieczeństwa miękkiego" opartego nie tylko na systemach ochrony, ale również na samej architekturze przestrzeni.

Znaczenie mają:

- dobre oświetlenie,
- widoczność ciągów komunikacyjnych,
- odpowiednie rozmieszczenie kamer,
- naturalna kontrola społeczna przestrzeni,
- czytelny podział stref publicznych i prywatnych,
- projektowanie przestrzeni ograniczających anonimowość.

To podejście bardzo dobrze wpisuje się w globalny trend *human-centric design,* w którym bezpieczeństwo ma być naturalnym elementem jakości życia mieszkańców, a nie wyłącznie systemem kontroli.

Nowoczesne inwestycje mieszkaniowe i komercyjne są dziś znacznie bardziej zaawansowane technologicznie niż jeszcze dekadę temu. Inteligentne budynki zarządzają energią, wentylacją, dostępem, monitoringiem, parkingami i komunikacją wewnętrzną. Problem polega na tym, że wraz z cyfryzacją rośnie również skala potencjalnych zagrożeń.

Deweloperzy coraz częściej muszą myśleć nie tylko o ochronie fizycznej budynku, ale również o:

- cyberbezpieczeństwie systemów budynkowych,
- odporności infrastruktury energetycznej,
- bezpieczeństwie danych mieszkańców,
- ciągłości działania systemów automatyki,
- ochronie przed sabotażem i zakłóceniami operacyjnymi.

To szczególnie istotne w dużych inwestycjach *mixed-use*, które zaczynają funkcjonować jak małe organizmy miejskie. Awaria systemów bezpieczeństwa, zasilania czy kontroli dostępu może wpływać na codzienne funkcjonowanie tysięcy ludzi. W efekcie rynek nieruchomości coraz mocniej zbliża się dziś do rynku infrastruktury krytycznej.

Deweloperzy coraz częściej konkurują bezpieczeństwem

Zmienia się również sam język rynku nieruchomości. Jeszcze kilka lat temu inwestycje mieszkaniowe sprzedawano głównie lokalizacją, metrażem i standardem wykończenia. Dziś coraz większą rolę odgrywa jakość życia, a jej fundamentem bardzo często staje się właśnie bezpieczeństwo.

Mieszkańcy zwracają uwagę nie tylko na estetykę inwestycji, ale również na:

- poziom prywatności,
- bezpieczeństwo dzieci,
- ochronę części wspólnych,
- komfort poruszania się po osiedlu,
- bezpieczeństwo dostaw i przesyłek,
- dostępność terenów zielonych,
- jakość przestrzeni publicznych.

Obiekty użyteczności publicznej muszą być dziś odporne

Nowoczesne miasta działają dzięki miejscom, których większość mieszkańców na co dzień nawet nie zauważa. Szpitale, dworce, urzędy, szkoły, centra transportowe, stadiony, tunele, obiekty administracji czy infrastruktura komunalna tworzą system naczyń połączonych, od których zależy codzienne funkcjonowanie miasta. Przez lata bezpieczeństwo tych obiektów kojarzyło się głównie z ochroną fizyczną: kontrolą wejść, monitoringiem czy obecnością służb ochrony. Dziś to zdecydowanie za mało.

Współczesne obiekty użyteczności publicznej stają się coraz bardziej zależne od technologii, automatyki i ciągłości działania systemów cyfrowych. Jednocześnie rośnie liczba zagrożeń, które mogą wpływać na ich funkcjonowanie – od cyberataków i przeciążeń infrastruktury po sabotaż, blackouty czy sytuacje kryzysowe związane z bezpieczeństwem publicznym.

W efekcie miasta coraz częściej zaczynają myśleć o takich obiektach nie tylko w kategorii „budynków", ale elementów infrastruktury odpornościowej całego miasta.

Bezpieczeństwo to dziś ciągłość działania

do niedawna większość systemów security projektowano głównie wokół reagowania na incydenty. Współczesne podejście wygląda inaczej. Kluczowym pojęciem

staje się dziś *operational resilience,* czyli zdolność obiektu do utrzymania działania nawet w sytuacji zakłóceń. To ogromna zmiana filozofii. Szpital nie może przestać działać podczas awarii zasilania. Dworzec musi funkcjonować mimo przeciążenia systemów. Centrum zarządzania ruchem nie może utracić dostępu do danych. Budynek administracji publicznej musi zachować możliwość komunikacji nawet podczas cyberincydentu.

Nowoczesne security coraz częściej oznacza więc:

- redundancję systemów,
- odporność infrastruktury IT,
- bezpieczeństwo energetyczne,
- procedury kryzysowe,
- integrację różnych systemów zarządzania,
- szybkie wykrywanie anomalii,
- zdolność do działania w warunkach kryzysowych.

To szczególnie ważne w świecie, w którym granica między zagrożeniami fizycznymi i cyfrowymi praktycznie przestaje istnieć.

Współczesny obiekt użyteczności publicznej jest dziś połączonym organizmem technologicznym. Systemy monitoringu wizyjnego, kontroli dostępu, alarmowe, wentylacji, energetyki, transportu i komunikacji funkcjonują coraz częściej w jednej wspólnej infrastrukturze. Problem polega na tym, że ta integracja tworzy również nowe ryzyka. Cyberatak na system automatyki budynkowej może dziś wpływać na działanie kontroli dostępu. Awaria sieci może ograniczyć możliwości monitoringu. Zakłócenie systemów komunikacyjnych może sparaliżować zarządzanie kryzysowe obiektu. Dlatego współczesne miasta coraz częściej odchodzą od podziału na *security fizyczne* i *cybersecurity*. Oba obszary zaczynają funkcjonować jako wspólny system bezpieczeństwa operacyjnego.

W praktyce oznacza to rosnące znaczenie:

- integracji systemów bezpieczeństwa,
- centralnych platform zarządzania,
- analizy danych w czasie rzeczywistym,
- monitorowania infrastruktury technicznej,
- inteligentnej automatyki reagowania,
- systemów komunikacji kryzysowej.

Coraz częściej nie chodzi już wyłącznie o ochronę obiektu, ale o zdolność przewidywania zagrożeń i ograniczania skutków incydentów zanim wpłyną na funkcjonowanie miasta.

Dworce, szpitale i stadiony stają się „żywymi organizmami”

Najbardziej widoczne jest to w dużych obiektach publicznych o wysokim poziomie złożoności operacyjnej. Nowoczesny dworzec kolejowy czy stadion funkcjonuje dziś jak małe miasto – z własnym ruchem, logistyką, komunikacją, energetyką i bezpieczeństwem. Zmiana podejścia do bezpieczeństwa obiektów użyteczności publicznej jest również efektem szerszych zmian geopolitycznych i społecznych. Pandemia, wojna w Europie, rosnąca liczba cyberataków, kryzysy energetyczne i coraz częstsze ekstremalne zjawiska pogodowe sprawiły, że miasta zaczęły myśleć o bezpieczeństwie w sposób znacznie bardziej strategiczny.

Jeszcze kilka lat temu wiele zagrożeń traktowano jako mało prawdopodobne scenariusze kryzysowe. Dziś stają się częścią codziennego planowania operacyjnego. Samorządy, operatorzy infrastruktury i zarządcy obiektów publicznych coraz częściej muszą odpowiadać na pytania:

- jak utrzymać działanie miasta podczas blackoutów,
- jak chronić systemy transportowe,
- jak zabezpieczać dane mieszkańców,
- jak reagować na przeciążenia infrastruktury,
- jak zarządzać bezpieczeństwem podczas masowych ewakuacji,
- jak ograniczać skutki cyberataków,
- jak komunikować się z mieszkańcami podczas kryzysu.

Nowoczesne miasto nie musi już udowadniać swojej innowacyjności. To właśnie dlatego współczesne smart city coraz bardziej oddala się od swojej pierwotnej definicji. Inteligentne miasto nie jest dziś zbiorem technologicznych rozwiązań. Jest sposobem myślenia o przestrzeni, mieszkańcach i odporności miasta na zmieniający się świat.

Oczekiwania wobec przestrzeni miejskiej są znacznie bardziej pragmatyczne niż jeszcze dekadę temu. Ludzie chcą mieszkać w miejscach wygodnych, bezpiecznych, spokojnych i dobrze zorganizowanych. Coraz większe znaczenie mają lokalność, dostępność usług, jakość przestrzeni wspólnych, zieleń i poczucie codziennego komfortu. I być może najciekawsze jest dziś właśnie to, że najbardziej nowoczesne miasta wcale nie próbują wyglądać nowocześnie. Zamiast tego starają się tworzyć przestrzenie, w których mieszkańcy po prostu czują, że miasto działa dla nich. Spokojnie, bezpiecznie i przewidywalnie. •

Redakcja „a&s Polska”

Ilustracje: Marta Kołodziejak / A&S AI Studio

Europa przyspiesza wdrażanie dozoru opartego na AI

Inteligentne bezpieczeństwo w erze smart city – analiza rynku do 2030 roku

Sztuczna inteligencja przestaje być jedynie wsparciem dla systemów bezpieczeństwa – staje się ich fundamentem. W Europie obserwujemy wyraźne przyspieszenie wdrażania zaawansowanych systemów monitoringu wizyjnego opartych na AI, które redefiniują sposób zarządzania bezpieczeństwem publicznym, infrastrukturą krytyczną oraz ruchem miejskim. Rozwiązania te stają się integralnym elementem transformacji cyfrowej europejskich miast i jednym z filarów rozwoju koncepcji smart city.

Nowa generacja dozoru wizyjnego

Największe ośrodki miejskie w Niemczech, Francji i Wielkiej Brytanii już dziś wdrażają rozwiązania określane mianem inteligentnego dozoru. Systemy te wykorzystują analitykę predykcyjną, rozpoznawanie wzorców zachowań oraz mechanizmy alertów w czasie rzeczywistym.

Dzięki temu służby mogą nie tylko reagować na incydenty, ale coraz częściej również przewidywać zagrożenia, zanim do nich dojdzie. Oznacza to fundamentalną zmianę modelu funkcjonowania systemów bezpieczeństwa – przejście od bezpieczeństwa reaktywnego do proaktywnego.

Nowoczesny monitoring oparty na AI umożliwia automatyczne wykrywanie niebezpiecznych zdarzeń, identyfikację anomalii czy analizę zachowań tłumu. W praktyce systemy te wspierają działania policji, straży miejskiej, operatorów transportu publicznego oraz centrów zarządzania kryzysowego, znacząco zwiększając skuteczność reagowania i koordynacji działań operacyjnych.

Rynek w fazie dynamicznego wzrostu

Europejski sektor monitoringu AI znajduje się obecnie w fazie intensywnej ekspansji. Według analiz MarketsandMarkets wartość rynku osiągnęła około 3,90 mld USD w 2024 roku, a prognozy wskazują na wzrost do 12,46 mld USD do 2030 roku.

Średnioroczne tempo wzrostu (CAGR) na poziomie 21,3% pokazuje, że technologie dozoru opartego na sztucznej inteligencji stają się jednym z najważniejszych segmentów branży security.

Za dynamicznym wzrostem rynku stoją przede wszystkim:

- rosnące inwestycje publiczne w technologie AI,
- zwiększone wymagania dotyczące bezpieczeństwa publicznego,
- rozwój infrastruktury smart city,
- postęp technologiczny w obszarze analizy obrazu i danych,
- potrzeba ochrony infrastruktury krytycznej oraz systemów transportowych.

Wzrost znaczenia monitoringu AI wynika również z rosnącej presji na zwiększanie efektywności działania służb miejskich przy jednoczesnym ograniczaniu kosztów operacyjnych. Inteligentne systemy nadzoru pozwalają automatyzować wiele procesów analitycznych i znacząco odciążać operatorów centrów monitoringu.

Technologie zmieniające reguły gry

Rozwój europejskiego rynku monitoringu AI napędzają konkretne innowacje technologiczne, które zwiększają skuteczność oraz skalowalność systemów bezpieczeństwa.

Kluczowe znaczenie mają:

- rozpoznawanie twarzy i identyfikacja biometryczna,
- *edge computing* umożliwiający analizę danych bezpośrednio na urządzeniach,
- sieci neuronowe analizujące obraz w czasie rzeczywistym,
- automatyczna analiza zachowań i wykrywanie anomalii,
- integracja monitoringu z platformami IoT i systemami miejskimi.

Połączenie tych technologii pozwala znacząco skrócić czas reakcji na incydenty oraz zwiększyć skuteczność wykrywania zagrożeń. Coraz większą rolę odgrywa *edge AI,* które umożliwia przetwarzanie danych bezpośrednio w kamerach lub urządzeniach brzegowych, ograniczając obciążenie centralnych systemów IT i poprawiając wydajność infrastruktury monitoringu.

Jednocześnie rozwój sztucznej inteligencji powoduje, że monitoring staje się coraz bardziej autonomiczny. Systemy potrafią samodzielnie klasyfikować zdarzenia, filtrować fałszywe alarmy oraz priorytetyzować sytuacje wymagające interwencji człowieka.

Smart city jako katalizator zmian

Rozwój koncepcji smart city w Europie jest jednym z najważniejszych czynników napędzających wdrażanie inteligentnych systemów monitoringu. Współczesne miasta traktują dane jako strategiczny zasób umożliwiający efektywniejsze zarządzanie przestrzenią miejską, bezpieczeństwem oraz usługami publicznymi.

Monitoring wizyjny przestaje pełnić wyłącznie funkcję pasywnej rejestracji zdarzeń, a staje się aktywnym elementem infrastruktury miejskiej wspierającym procesy decyzyjne w czasie rzeczywistym. Samorządy integrują systemy dozoru z infrastrukturą Internetu Rzeczy (IoT), sieciami sensorów, platformami analitycznymi oraz miejskimi centrami zarządzania.

W praktyce oznacza to:

- lepszą koordynację działań służb miejskich i ratunkowych,
- automatyczne wykrywanie incydentów i zagrożeń,
- optymalizację ruchu drogowego,
- inteligentne sterowanie sygnalizacją świetlną,
- automatyzację procedur reagowania kryzysowego,
- poprawę efektywności transportu publicznego.

Zaawansowane algorytmy analityczne umożliwiają szybkie wykrywanie sytuacji kryzysowych, takich jak wypadki drogowe, pożary, akty wandalizmu czy wtargnięcia do stref chronionych. Informacje te mogą być natychmiast przekazywane odpowiednim służbom, co znacząco skraca czas reakcji i poprawia skuteczność interwencji.

Ilustracje: Marta Kołodziejak / A&S AI Studio

Wraz z rozwojem inteligentnych miast rośnie również zapotrzebowanie na skalowalne i interoperacyjne platformy monitoringu zdolne do integracji z wieloma źródłami danych i obsługi ogromnych wolumenów informacji w czasie rzeczywistym.

Regulacje jako motor odpowiedzialnych innowacji

Europa wyróżnia się na tle innych regionów szczególnie silnym podejściem do ochrony prywatności i danych osobowych. Regulacje, takie jak RODO (GDPR) oraz rozwijane przepisy dotyczące sztucznej inteligencji wyznaczają ramy dla funkcjonowania systemów monitoringu opartych na sztucznej inteligencji.

Choć regulacje bywają postrzegane jako ograniczenie rozwoju technologii, w praktyce stają się istotnym katalizatorem innowacji. Wymuszają projektowanie systemów transparentnych, bezpiecznych oraz zgodnych z zasadą *privacy-by-design*.

W rezultacie rozwijane są rozwiązania obejmujące między innymi:

- anonimizację danych,
- automatyczne maskowanie wizerunku,
- ograniczenie zakresu przechowywania informacji,
- transparentność działania algorytmów,
- zwiększone standardy cyberbezpieczeństwa.

Europejski model rozwoju monitoringu AI opiera się więc nie tylko na efektywności technologicznej, ale również na budowaniu społecznego zaufania oraz ochronie praw obywatelskich.

Perspektywy do 2030 roku

Do końca obecnej dekady europejski rynek monitoringu i dozoru opartego na sztucznej inteligencji będzie należał do najszybciej rozwijających się segmentów branży security. Dynamiczna urbanizacja, rozwój smart city, rosnące znaczenie cyberbezpieczeństwa oraz potrzeba zwiększania odporności infrastruktury krytycznej będą napędzać dalsze inwestycje w inteligentne systemy nadzoru.

W kolejnych latach można spodziewać się:

- dalszej integracji AI z infrastrukturą miejską,
- rozwoju analityki predykcyjnej,
- wzrostu znaczenia *edge AI*,
- popularyzacji technologii *privacy-by-design*,
- rosnącej roli współpracy publiczno-prywatnej,
- rozwoju interoperacyjnych platform bezpieczeństwa.

Szczególnego znaczenia nabierze analityka predykcyjna, która pozwoli systemom monitoringu identyfikować wzorce zachowań oraz przewidywać potencjalne zagrożenia jeszcze przed ich wystąpieniem. Monitoring stanie się coraz bardziej autonomiczny i będzie pełnił funkcję aktywnego narzędzia wspierającego zarządzanie miastem.

Jednocześnie europejski sektor monitoringu będzie musiał mierzyć się z wyzwaniami związanymi z ochroną prywatności i praw obywatelskich. Rozwój technologii rozpoznawania twarzy, analizy behawioralnej czy automatycznej identyfikacji osób będzie wymagał utrzymania równowagi pomiędzy bezpieczeństwem publicznym a ograniczaniem ryzyka nadużyć i nadmiernej inwigilacji.

W perspektywie długoterminowej monitoring oparty na sztucznej inteligencji stanie się jednym z fundamentów funkcjonowania inteligentnych miast w Europie. Jego rola będzie wykraczać poza tradycyjnie rozumiane bezpieczeństwo, obejmując również wsparcie polityki transportowej, ochrony środowiska, planowania urbanistycznego oraz zarządzania kryzysowego.

Europa rozwija tym samym własny model inteligentnego dozoru oparty na połączeniu innowacyjności technologicznej, wysokich standardów etycznych oraz odpowiedzialnego zarządzania danymi. To właśnie ten model może w najbliższych latach stać się globalnym wzorcem rozwoju nowoczesnych systemów monitoringu AI. •

Redakcja „a&s Polska”

AI w monitoringu to już standard.

O przewadze decyduje architektura platformy

Smart city przeszło z fazy zachłyśnięcia się technologią do fazy dojrzałości. Wiemy już, co realnie się sprawdza, a co było jedynie ideą. Tym, co dziś różnicuje projekty w tym obszarze, są architektura i bezpieczeństwo systemu.

Magdalena Hajdysz

Inteligentne bezpieczeństwo to zaplanowany scenariusz, a nie automat

Przez ostatnią dekadę analityka generowała głównie alerty, które operator musiał obsługiwać ręcznie. Dojrzała analityka działa inaczej: już milisekundy po zdarzeniu operator otrzymuje jego wielowątkowy kontekst i gotowy do uruchomienia scenariusz reakcji. Decyzja nadal należy do człowieka – zasada *human-in-the-loop* nie podlega negocjacji i wynika wprost z art. 14 AI Act dotyczącego systemów wysokiego ryzyka, do których zaliczają się również niektóre zastosowania w przestrzeni publicznej. Skraca się natomiast czas potrzebny na podjęcie decyzji – z minut do sekund.

W praktyce wygląda to następująco:

- Tłum gęstnieje przy bramce podczas imprezy miejskiej. Algorytm liczy osoby, a operator otrzymuje powiększony widok strefy oraz listę działań możliwych do uruchomienia jednym kliknięciem, np. otwarcie kolejnej bramki, komunikat na tablicy LED czy informację do służb. Operator weryfikuje sytuację i potwierdza decyzję.
- Poszukiwany pojazd mija kamerę ANPR, system natychmiast wyświetla punkt rejestracji, kolejne kamery na trasie oraz propozycję powiadomienia patrolu.
- Pożar w szkole – system pokazuje strefę zagrożenia, a moduł *musteringu* (elektronicznej ewidencji osób w punktach zbiórki) liczy uczniów oraz pracowników szkoły. Operator otrzymuje gotowy komunikat ewakuacyjny do nadania przez głośniki IP.

Człowiek zachowuje ostatnie słowo, a każda decyzja zostaje udokumentowana zgodnie z obowiązującymi przepisami.

Jeden pulpit zamiast kilkunastu aplikacji

Dojrzała architektura miejska wymaga już czegoś więcej niż klasycznego VMS. Potrzeba platformy, która w jednym widoku integruje kamery, kontrolę dostępu, czujniki pożarowe, stacje pogodowe, parkingi, ANPR, trasy patroli a także dwustronną komunikację z mieszkańcami. Docelowo to również jeden rejestr zdarzeń, jeden łańcuch dowodowy i jeden ślad audytowy.

Im więcej AI pojawia się w urządzeniach czy systemach, tym większa dyscyplina musi panować w warstwie zarządzania. Audyty związane z NIS2/ustawą o KSC oraz RODO pytają o konkrety: mapę przetwarzania danych, politykę retencji, plan reagowania na incydenty czy dokumentację scenariuszy działania. Dojrzała platforma generuje większość tych elementów automatycznie. Równie istotnym wymogiem rynku pozostaje otwartość – platforma musi współpracować z infrastrukturą, która już działa w mieście, najlepiej niezależnie od producenta urządzeń.

Civileo 2.0 – polska odpowiedź na dojrzewający rynek

Civileo Smart City 2.0 powstało z myślą właśnie o tym etapie rozwoju rynku. To polski VMS nowej generacji, integrujący dane z urządzeń różnych producentów i łączący w jednym pulpicie – w skali największych wdrożeń miejskich w Europie – kamery, dane z czujników środowiskowych, natężenie ruchu, kontrolę dostępu, parkingi, alarmy, *mustering*, komunikację głosową przez głośniki IP oraz powiadomienia dla mieszkańców. System zapewnia przy tym automatyczną dokumentację zdarzeń i zgodność z polskimi oraz unijnymi regulacjami.

Tam, gdzie standardowa analityka okazuje się niewystarczająca, Civileo umożliwia budowę dedykowanych modeli AI do analizy obrazu i dźwięku, projektowanych pod konkretne potrzeby danego miasta. Dojrzałe smart city nie wybiera już między dobrą architekturą a skutecznym algorytmem. Potrzebuje obu tych elementów w jednym miejscu, z człowiekiem pozostającym w centrum procesu decyzyjnego.

Klasyfikacja obiektów – pojazdów i osób, czy ANPR stały się branżowym standardem. Dynamicznie rozwijane są zaawansowane algorytmy detekcji obiektów po cechach szczególnych: kolorach, napisach, znakach graficznych oraz analiza zdarzeń dźwiękowych czy wyszukiwanie językiem naturalnym.

Jednak to, co dziś naprawdę różnicuje projekty smart city, leży gdzie indziej: w architekturze platformy oraz jej bezpieczeństwie. •

OKE Poland
ul. Jana z Kolna 11, 80-864 Gdańsk
Tel. +48 691 082 277
www.oke.pl

Sekundy, które decydują o bezpieczeństwie

Bezpieczeństwo w obiektach o dużym natężeniu ruchu staje się jednym z kluczowych wyzwań współczesnego zarządzania nieruchomościami. Dotyczy to zarówno przestrzeni edukacyjnych, biurowych, galerii handlowych, osiedli mieszkaniowych, jak i węzłów komunikacyjnych czy obiektów użyteczności publicznej.

Tradycyjne systemy zabezpieczeń – choć nadal stanowią fundament ochrony obiektów – nie zawsze zapewniają wystarczająco szybką reakcję w sytuacjach kryzysowych. Monitoring wizyjny umożliwia rejestrowanie i analizowanie zdarzeń, jednak nie zapewnia użytkownikowi prostego i bezpośredniego sposobu wezwania pomocy.

W odpowiedzi na te wyzwania Seris Konsalnet rozwija system **Help Point** – rozwiązanie umożliwiające bezpośrednie i natychmiastowe połączenie ze służbami odpowiedzialnymi za bezpieczeństwo obiektu.

Gdy liczy się czas reakcji

Zarządzanie bezpieczeństwem w przestrzeniach publicznych obejmuje szerokie spektrum zdarzeń: od incydentów porządkowych, takich jak kradzieże czy akty agresji, po nagłe sytuacje zdrowotne: zasłabnięcia, wypadki czy zagrożenia wymagające natychmiastowej interwencji.

W praktyce największym wyzwaniem nie zawsze jest brak środków komunikacji, lecz okoliczności towarzyszące zdarzeniu – stres, dezorientacja, presja czasu czy trudność w precyzyjnym przekazaniu lokalizacji.

Help Point odpowiada na te problemy poprzez maksymalne uproszczenie procesu zgłoszenia. System opiera się na intuicyjnym urządzeniu wyposażonym w jeden, wyraźnie oznaczony przycisk alarmowy. Jego naciśnięcie inicjuje natychmiastowe połączenie głosowe z wcześniej zdefiniowanym punktem kontaktowym – może to być centrum monitoringu, recepcja, ochrona obiektu lub odpowiednie służby.

Rozwiązanie działa całodobowo i nie wymaga instalowania aplikacji ani znajomości numerów alarmowych. Dzięki temu znacząco skraca czas od wystąpienia zdarzenia do rozpoczęcia interwencji.

Technologia, która uzupełnia istniejące systemy

Pierwsze wdrożenia Help Point funkcjonują już w praktyce. System został zainstalowany m.in. w jednej z warszawskich uczelni wyższych, gdzie urządzenia rozmieszczono w kluczowych punktach komunikacyjnych budynku, zapewniając szybki dostęp do pomocy w miejscach o największym natężeniu ruchu.

Współczesne systemy bezpieczeństwa coraz częściej ewoluują w kierunku modeli hybrydowych, łączących obserwację, analizę i szybką interwencję. Help Point wpisuje się w ten model, pełniąc funkcję „punktu pierwszego kontaktu" w sytuacjach kryzysowych.

Odporność i niezawodność w przestrzeni publicznej

Help Point został zaprojektowany do instalacji zarówno wewnętrznych, jak i zewnętrznych. Obudowa urządzeń zapewnia odporność na zmienne warunki atmosferyczne oraz akty wandalizmu, co umożliwia ich długoterminowe użytkowanie w przestrzeni publicznej.

System może działać jako rozwiązanie autonomiczne lub zostać zintegrowany z istniejącą infrastrukturą bezpieczeństwa. Dzięki temu znajduje zastosowanie w wielu typach obiektów – od centrów handlowych i biurowców, przez osiedla mieszkaniowe, aż po placówki medyczne, kampusy edukacyjne i przestrzenie transportowe.

Dostępność jako standard bezpieczeństwa

Help Point został wyposażony w pętlę indukcyjną wspierającą komunikację osób niedosłyszących, a jego konstrukcja i sposób montażu uwzględniają potrzeby osób poruszających się na wózkach oraz innych grup o szczególnych wymaganiach.

Jak podkreślają eksperci Seris Konsalnet: *Skuteczny system bezpieczeństwa musi być intuicyjny i dostępny dla każdego użytkownika przestrzeni, niezależnie od jego sytuacji czy ograniczeń. Projektując Help Point, skupiliśmy się na maksymalnym uproszczeniu obsługi i eliminacji barier, które w sytuacjach kryzysowych mogą decydować o czasie reakcji. W takich momentach każda sekunda ma znaczenie.*

Rosnące oczekiwania wobec zarządców nieruchomości oraz operatorów obiektów sprawiają, że sama obecność systemów zabezpieczeń przestaje być wystarczająca. Kluczowe stają się dziś ich funkcjonalność, integracja oraz zdolność do szybkiego działania.

Rozwiązania, takie jak Help Point, odpowiadają na potrzebę skracania czasu reakcji i zwiększania dostępności pomocy w sytuacjach kryzysowych. •

SERIS KONSALNET
ul. Jana Kazimierza 55
01-267 Warszawa
www.seris.pl

Wielkoskalowe modele AI w systemach Smart City

Sztuczna inteligencja oparta na nowoczesnych wielkoskalowych modelach to zaawansowana technologia, która rewolucjonizuje koncepcję Smart City, integrując inteligentne rozwiązania AIoT z infrastrukturą miejską. **Firma Hikvision** opracowała w tym zakresie technologię Guanlan, której nazwa nawiązuje do starożytnej filozofii mówiącej, że zrozumienie natury wymaga uważnej obserwacji zjawisk.

Tomasz Goljaszewski

Technologia Guanlan opiera się na trójwarstwowej architekturze, obejmującej:

- warstwę podstawową: modele wizyjne, językowe i multimodalne;
- warstwę pośrednią: modele branżowe, zbudowane z udziałem fachowej wiedzy z zakresu konkretnej branży oraz specyfiki występujących w niej przypadków;
- najwyższą warstwę: złożone modele zadaniowe opracowane dla szczególnych przypadków, w których potrzebna jest analiza modeli warstwy podstawowej i pośredniej w konkretnych scenariuszach oraz zależnościach.

W przypadku wcześniej wspomnianych modeli multimodalnych w warstwie podstawowej, oprócz modeli wizyjnych możemy mieć do czynienia z dużymi modelami dla termowizji, modelami fal milimetrowych (radary), modelami światłowodowymi (analizatory) oraz modelami fal rentgenowskich (bramki, skanery). Wszystkie te technologie można integrować z zewnętrznymi systemami i zarządzać nimi centralnie w ramach wielkoskalowych projektów ochrony aglomeracji.

AI w nowoczesnym monitoringu miejskim

Obecnie wielkoskalowe modele AI są najczęściej wykorzystywane w kilku obszarach związanych z bezpieczeństwem i funkcjonowaniem miasta. Jednym z nich jest system monitoringu miejskiego. Zastosowanie tej nowoczesnej technologii umożliwia błyskawiczne wyszukiwanie zdarzeń w zarejestrowanym materiale za pomocą opisów tekstowych. Ponieważ wielkoskalowe modele AI rozumieją cechy obiektów oraz kontekst, umożliwiają szybkie wyszukiwanie obiektów przy użyciu tekstowych instrukcji wysyłanych do urządzeń systemowych.

Stosując tekstowe opisy jako polecenia wyszukiwania, np. „kobieta z wózkiem dziecięcym" czy „człowiek prowadzący psa", jesteśmy w stanie bardzo szybko odnaleźć w zarejestrowanych danych interesujące nas nagranie. Kluczowe dla tej funkcjonalności są wielkoskalowe modele językowe Guanlan oraz funkcja AcuSeek, zaimplementowana w kamerach i rejestratorach Hikvision. Inteligentne rejestratory DeepinMind z funkcją AcuSeek (seria Vpro), wraz z platformą systemową HikCentral Pro, stanowią podstawę działania takiego systemu.

W przypadku dużych systemów Hikvision zapewnia serwery AI z serii Fusion Ultra, które mają dzienną wydajność detekcji do 3 mln obiektów (wskaźnik podano dla kamer Full HD). W takim przypadku rejestracja nie odbywa się na rejestratorach, lecz na macierzach dedykowanych systemowi HikCentral Pro.

Ochrona infrastruktury krytycznej z wykorzystaniem AI

Kolejnym istotnym obszarem, w którym wdrożono sztuczną inteligencję opartą na wielkoskalowych modelach AI, jest ochrona obiektów istotnych z punktu widzenia funkcjonowania miasta. Mogą to być obiekty strategiczne, takie jak dworce, duże węzły komunikacyjne, zakłady produkcji czystej wody czy obiekty związane z produkcją i dystrybucją energii elektrycznej oraz ciepła.

Algorytmy detekcji działające w oparciu o Guanlan znacząco podnoszą efektywność wykrywania zagrożeń. Na przykład w przypadku detekcji człowieka skuteczność wzrasta o 5–10%, w zależności od dystansu czy rozdzielczości kamery. Z kolei w przypadku

innych obiektów, np. pozostawionego przedmiotu czy obecności dymu, skuteczność jest wyższa – od kilkunastu do kilkudziesięciu procent.

Wzrost skuteczności może przekładać się na większe zasięgi detekcji oraz redukcję liczby fałszywych alarmów. Redukcja fałszywych alarmów jest szczególnie istotna z punktu widzenia pracy operatorów systemów bezpieczeństwa. Ma ona podstawowy wpływ na efektywność detekcji oraz czas reakcji na zagrożenie.

Hikvision wprowadziło specjalną serię kamer wizyjnych i termowizyjnych, w których algorytmy detekcji zostały usprawnione właśnie dzięki wielkoskalowym modelom AI. Technologię Guanlan można znaleźć w wybranych kamerach 5. i 7. linii oraz kamerach termowizyjnych linii G1.

Sztuczna inteligencja w zarządzaniu ruchem drogowym

Ważnym obszarem, w którym wykorzystuje się wielkoskalowe modele AI, są drogi miejskie, a co za tym idzie – wykrywanie zagrożeń w ruchu drogowym. Zarządzanie ruchem drogowym z wykorzystaniem wielkoskalowych modeli AI, w połączeniu z systemami ITS, ma na celu zwiększenie bezpieczeństwa na drogach miejskich. Dodatkowo technologie te wpływają na optymalizację przepływu pojazdów oraz redukcję liczby fałszywie wykrytych wykroczeń i incydentów drogowych.

Ze względu na zdecydowanie wyższą skuteczność wykrywania w porównaniu z tradycyjnymi systemami bazującymi na typowej analizie wideo, mogą służyć do dyscyplinowania kierowców i wymuszania poprawnych zachowań na użytkownikach dróg. Badania wykazały, że stosowanie wielkoskalowych modeli AI (zwłaszcza wykorzystujących warstwę pośrednią, czyli modele branżowe) do wykrywania wykroczeń, takich jak jazda pod prąd, skręt z niewłaściwego pasa ruchu, zajmowanie buspasa, brak zapiętych pasów czy używanie telefonu podczas jazdy, umożliwia redukcję fałszywych alarmów nawet o 75%, jednocześnie zwiększając skuteczność odczytu numerów rejestracyjnych do 98%, a cech pojazdu do 95%.

Nowa generacja kamer ANPR

Firma Hikvision, wykorzystując technologię Guanlan, opracowała w zeszłym roku nowe kamery ANPR przeznaczone do zastosowania na drogach szybkiego ruchu oraz drogach miejskich. Kamery te oferują lepszą skuteczność nie tylko w zakresie funkcji podstawowych (czyli odczytu tablic rejestracyjnych), lecz także funkcji dodatkowych, takich jak detekcja koloru, cech pojazdu, prędkości czy niektórych wykroczeń.

Oprócz kamer ANPR gamę produktów uzupełniły również nowe kamery do detekcji i monitorowania przepływu pojazdów *(Traffic Flow)* oraz detekcji incydentów (AID). We wszystkich tych produktach zastosowano wielkoskalowe modele AI w warstwie podstawowej i pośredniej, a w niektórych przypadkach również w warstwie zadaniowej.

Przyszłość AI w przestrzeni miejskiej

W przyszłości wielkoskalowe modele AI będą coraz częściej wykorzystywane w różnych obszarach życia miasta w celu zwiększania efektywności oraz automatyzacji procesów. Takie problemy, jak parkowanie w mieście, zbiórka śmieci czy bezpieczeństwo dzieci w drodze do szkoły mogą być kolejnymi obszarami, w których można zaimplementować technologie bazujące na AI.

Wraz ze wzrostem popularności technologii termowizyjnej, radarowej czy innych technologii niewizyjnych (np. światłowodów) wzrośnie również znaczenie modeli multimodalnych. Z całą pewnością technologia ta nie jest jedynie krótkotrwałym trendem. Należy się spodziewać, że na stałe wpisze się w definicję systemów Smart City. Wszystko to z korzyścią dla nas, czyli zwykłych mieszkańców miast i użytkowników infrastruktury miejskiej. •

Hikvision Poland
ul. Żwirki i Wigury 16B
02-092 Warszawa
www.hikvision.com/europe/
info.pl@hikvision.com

Inteligentne miasta mówią ludzkim głosem

Transformacja miast w kierunku koncepcji smart city przyspiesza. Władze miejskie inwestują w technologie, które mają poprawić bezpieczeństwo, ograniczyć zanieczyszczenie i podnieść komfort życia mieszkańców. Jednak wraz z rozwojem infrastruktury pojawiają się nowe wyzwania operacyjne.

Jednym z kluczowych problemów staje się skuteczna komunikacja – szczególnie w sytuacjach kryzysowych. Rosnąca liczba mieszkańców, przeciążone systemy transportowe oraz wielojęzyczność społeczności miejskich sprawiają, że przekazywanie jasnych i natychmiastowych informacji jest coraz trudniejsze. W tym kontekście kluczową rolę zaczynają odgrywać nie tylko systemy DSO jako całość, ale ich najbardziej „fizyczny" element – głośniki.

Systemy nagłośnienia jako aktywne narzędzie bezpieczeństwa

Współczesne systemy nagłośnienia w przestrzeni miejskiej przestały pełnić wyłącznie funkcję informacyjną. Stały się aktywnym elementem infrastruktury bezpieczeństwa, zdolnym do realnego wpływu na przebieg zdarzeń.

Zintegrowane z monitoringiem wizyjnym rozwiązania audio umożliwiają operatorom podejmowanie natychmiastowych działań. Komunikat głosowy nadany w czasie rzeczywistym często wystarczy, aby przerwać incydent – od wandalizmu po nielegalne działania w przestrzeni publicznej.

Coraz częściej systemy te współpracują z algorytmami sztucznej inteligencji. Automatyczna detekcja zdarzeń – takich jak krzyk czy tłuczone szkło – może inicjować emisję komunikatu bez udziału operatora.

Dźwiękowe systemy ostrzegawcze (DSO) w praktyce miejskiej

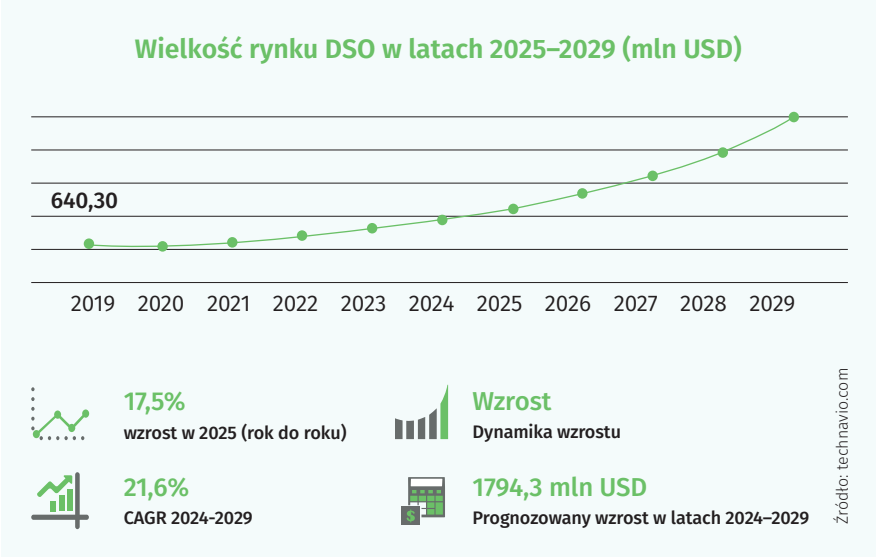
Dźwiękowe systemy ostrzegawcze (DSO) są dziś jednym z kluczowych elementów infrastruktury bezpieczeństwa w nowoczesnych miastach. Ich podstawową funkcją jest szybkie i skuteczne przekazywanie komunikatów alarmowych oraz instrukcji postępowania w sytuacjach zagrożenia – od pożarów i awarii technicznych po incydenty o charakterze terrorystycznym.

W przeciwieństwie do tradycyjnych systemów alarmowych DSO nie ograniczają się do sygnałów dźwiękowych. Umożliwiają emisję precyzyjnych komunikatów głosowych, co znacząco zwiększa skuteczność ewakuacji, redukuje panikę i pozwala lepiej kontrolować zachowanie tłumu.

Ich znaczenie wykracza jednak poza sytuacje kryzysowe. W codziennej eksploatacji wspierają zarządzanie ruchem pasażerskim, informowanie użytkowników przestrzeni publicznych oraz organizację przepływu ludzi w miejscach o dużym natężeniu ruchu, takich jak dworce, lotniska czy centra handlowe.

Prognozuje się, że wartość rynku dźwiękowych systemów ostrzegawczych wzrośnie o 1,79 mld USD, przy średniorocznym tempie wzrostu (CAGR) na poziomie 21,6% w latach 2024-2029.

Dzięki temu możliwe jest automatyczne uruchamianie scenariuszy alarmowych oraz dostosowywanie komunikatów do konkretnej sytuacji i lokalizacji. System może działać zarówno



Rynek odnotowuje znaczący postęp, napędzany integracją dźwiękowych systemów ostrzegawczych (DSO) ze sztuczną inteligencją (AI) i Internetem Rzeczy (IoT). Według badań rynkowych globalny rynek DSO będzie rósł w stałym tempie, ze szczególnym uwzględnieniem poprawy bezpieczeństwa i komunikacji w sytuacjach awaryjnych w różnych sektorach.

Przykładowo, przewiduje się znaczny wzrost w branży transportowej ze względu na coraz częstsze wdrażanie inicjatyw inteligentnych miast i integrację DSO z systemami transportu publicznego. Ponadto oczekuje się, że sektor opieki zdrowotnej również odnotuje znaczny wzrost, ponieważ systemy DSO zostaną zintegrowane ze szpitalami i placówkami opieki zdrowotnej, aby poprawić bezpieczeństwo pacjentów i usprawnić procedury reagowania kryzysowego.

Funkcjonalność i integracja

Nowoczesne systemy DSO są projektowane jako rozwiązania w pełni zintegrowane z miejskim ekosystemem technologicznym. W praktyce oznacza to współpracę z:

- systemami detekcji pożaru i zagrożeń,
- monitoringiem wizyjnym (CCTV),
- czujnikami IoT,
- platformami zarządzania kryzysowego.

w trybie automatycznym, jak i być sterowany ręcznie przez operatorów lub służby ratunkowe.

Wymagania techniczne i projektowe

Systemy DSO należą do infrastruktury krytycznej, dlatego ich projektowanie wymaga spełnienia rygorystycznych norm technicznych i jakościowych.

Kluczowe znaczenie ma zrozumiałość komunikatów, określana m.in. przez wskaźnik STI *(Speech Transmission Index)*. W przeciwieństwie do klasycznych systemów audio priorytetem nie jest jakość brzmienia, lecz czytelność przekazu – nawet w trudnych warunkach akustycznych.

Istotne są również:

- odporność urządzeń na warunki atmosferyczne i uszkodzenia mechaniczne,
- redundancja zasilania i infrastruktury,
- zgodność z normami (np. PN-EN 54),
- zdolność do pracy w warunkach awaryjnych.

System musi zachować pełną funkcjonalność nawet w przypadku częściowej awarii infrastruktury.

Rola DSO w zarządzaniu kryzysowym

W sytuacjach zagrożenia DSO pełnią funkcję nadrzędnego kanału komunikacji z użytkownikami przestrzeni miejskiej. Umożliwiają przekazywanie jasnych, aktualizowanych w czasie rzeczywistym instrukcji, co ma bezpośredni wpływ na skuteczność działań ratunkowych.

Dzięki nim służby mogą:

- kierować ewakuacją,
- dynamicznie zmieniać komunikaty w zależności od rozwoju sytuacji,
- ograniczać chaos informacyjny.

Efektem jest skrócenie czasu reakcji oraz zwiększenie bezpieczeństwa zarówno mieszkańców, jak i służb operacyjnych.

Wyzwania i kierunki rozwoju DSO

Wdrażanie systemów DSO wiąże się z określonymi wyzwaniami – przede wszystkim kosztami, koniecznością regularnych testów oraz integracją z istniejącą infrastrukturą miejską.

Jednocześnie kierunki rozwoju są jednoznaczne. Coraz większą rolę odgrywają:

- sztuczna inteligencja wspierająca analizę zdarzeń,
- automatyzacja komunikatów,
- personalizacja przekazu (np. językowa),
- integracja z urządzeniami mobilnymi.

W efekcie DSO ewoluują w stronę inteligentnych systemów komunikacji kryzysowej, które nie tylko reagują, ale również przewidują zagrożenia.

Wnioski: dźwięk jako filar inteligentnego miasta

Systemy audio, wspierane przez sztuczną inteligencję i zaawansowane technologie przetwarzania mowy, przestają być dodatkiem do infrastruktury miejskiej. Stają się jej integralnym i krytycznym komponentem.

W świecie rosnącej złożoności i dynamiki zagrożeń zdolność do szybkiej, zrozumiałej i wielojęzycznej komunikacji może decydować o skuteczności działań służb oraz bezpieczeństwie mieszkańców.

Inteligentne miasta przyszłości nie tylko „widzą" i „analizują" – ale przede wszystkim skutecznie komunikują się z ludźmi. •

Redakcja „a&s Polska"

Ilustracje: Marta Kołodziejak / A&S AI Studio

Mobilny monitoring wizyjny: od kosztu ochrony do narzędzia efektywności biznesowej

Mobilne wieże monitoringu jako nowy standard nowoczesnego security

Rynek mobilnego monitoringu wizyjnego dynamicznie rośnie, a jego znaczenie wykracza dziś daleko poza tradycyjnie rozumianą ochronę mienia. Transport, logistyka, budownictwo oraz sektor publiczny coraz częściej traktują mobilne systemy nadzoru jako element strategii operacyjnej łączący bezpieczeństwo, analitykę oraz optymalizację kosztów.

W

Według raportu MarketsandMarkets *Mobile Video Surveillance Market by Offering – Global Forecast to 2030,* globalny rynek mobilnego monitoringu wizyjnego wzrośnie z 2,78 mld USD w 2025 roku do 4,00 mld USD w 2030 roku, osiągając średnioroczne tempo wzrostu (CAGR) na poziomie 7,5%. To wyraźny sygnał, że mobilny monitoring przestał być rozwiązaniem niszowym i staje się jednym z kluczowych segmentów nowoczesnego rynku security.

Jednym z głównych motorów tego wzrostu są mobilne wieże monitoringu, odpowiadające na potrzebę szybkiego wdrażania ochrony w lokalizacjach pozbawionych stałej infrastruktury – na placach budowy, terenach inwestycyjnych, parkingach tymczasowych, w centrach logistycznych czy podczas wydarzeń masowych.

Widoczność, prewencja, reakcja w czasie rzeczywistym

Nowoczesny mobilny monitoring pełni dziś znacznie szerszą funkcję niż wyłącznie rejestracja obrazu. Autonomiczne wieże monitorujące stają się aktywnym elementem zarządzania bezpieczeństwem – odstraszają potencjalnych sprawców, zapewniają bieżący nadzór oraz umożliwiają natychmiastową reakcję na incydenty.

Ich dobrze widoczna konstrukcja działa prewencyjnie, ograniczając ryzyko kradzieży, wandalizmu czy sabotażu. Jednocześnie zastosowanie kamer PTZ, transmisji LTE/5G oraz integracji z centrami monitoringu pozwala operatorom reagować w czasie rzeczywistym, bez konieczności stałej obecności ochrony fizycznej.

AI DETECTION
Inteligentna analiza obrazu w czasie rzeczywistym

LIVE MONITORING
Podgląd na żywo z dowolnego miejsca 24/7

01 LOGISTYKA I TRANSPORT
Bezpieczne łańcuchy dostaw i infrastruktura

> W najbliższych latach mobilne systemy monitoringu będą coraz częściej pełnić funkcję inteligentnych, autonomicznych węzłów bezpieczeństwa – zintegrowanych z analityką AI, systemami smart city i zdalnym zarządzaniem operacyjnym.

5G / LTE CONNECT
Szybka transmisja danych i niezawodna łączność w każdych warunkach

REAL-TIME RESPONSE
Szybka reakcja i skuteczne zarządzanie incydentami

02 SMART CITY
Inteligentny monitoring przestrzeni miejskiej

03 IMPREZY MASOWE
Bezpieczeństwo uczestników i efektywne zarządzanie

W praktyce mobilne systemy dozoru:

- zapewniają szeroki obszar obserwacji z jednego punktu,
- eliminują konieczność budowy kosztownej infrastruktury kablowej,
- mogą być szybko relokowane wraz ze zmianą obszaru ryzyka,
- działają autonomicznie dzięki zasilaniu bateryjnemu lub solarnemu,
- integrują się z systemami VMS, VSaaS i platformami zarządzania bezpieczeństwem.

Dzięki temu doskonale sprawdzają się wszędzie tam, gdzie liczy się szybkie wdrożenie, elastyczność oraz skalowalność ochrony.

Logistyka i transport – bezpieczeństwo oraz efektywność operacyjna

Szczególnie dynamiczny rozwój mobilnego monitoringu obserwowany jest w logistyce i transporcie. Rosnąca liczba kradzieży ładunków, nieautoryzowanych wejść na teren terminali oraz coraz wyższe wymagania dotyczące odpowiedzialności operacyjnej powodują, że firmy poszukują bardziej elastycznych i ekonomicznych modeli ochrony.

Mobilne platformy monitoringu wykorzystywane są m.in. jako:

- tymczasowe punkty ochrony terminali logistycznych,
- zabezpieczenie parkingów flotowych i miejsc postoju,
- monitoring stref załadunku i rozładunku,
- wsparcie ochrony w okresach zwiększonego ryzyka operacyjnego.

Dla wielu organizacji oznacza to możliwość ograniczenia kosztów ochrony fizycznej przy jednoczesnym zwiększeniu skuteczności nadzoru. Pojedyncza wieża monitorująca może objąć dozorem rozległy obszar, zapewniając całodobową obserwację oraz zdalny dostęp do obrazu.

Model mobilny pozwala również uniknąć kosztownej budowy stałej infrastruktury w lokalizacjach tymczasowych. To szczególnie istotne w branżach, gdzie infrastruktura musi nadążać za dynamiką procesów logistycznych.

AI zmienia rolę mobilnego monitoringu

Jednym z najważniejszych trendów rynkowych jest integracja mobilnych systemów monitoringu z analityką obrazu opartą na sztucznej inteligencji. W efekcie mobilne wieże stają się nie tylko nośnikami kamer, ale także inteligentnymi punktami obserwacyjnymi aktywnie wspierającymi zarządzanie bezpieczeństwem.

Algorytmy AI umożliwiają m.in.:

- automatyczne wykrywanie intruzów,
- identyfikację naruszeń wyznaczonych stref,
- analizę nietypowych zachowań,
- śledzenie obiektów w ruchu,
- redukcję liczby fałszywych alarmów,
- priorytetyzację zdarzeń dla operatorów centrum nadzoru.

Dzięki temu operatorzy mogą szybciej identyfikować realne zagrożenia i efektywniej zarządzać incydentami. Monitoring przestaje być wyłącznie narzędziem archiwizacji obrazu – staje się źródłem danych operacyjnych wspierających podejmowanie decyzji.

Transport publiczny i infrastruktura tymczasowa

Transport publiczny pozostaje jednym z największych obszarów wykorzystania mobilnego monitoringu, jednak coraz większą rolę odgrywają także wdrożenia tymczasowe związane z modernizacją infrastruktury i organizacją ruchu.

Autonomiczne systemy dozorowe wykorzystywane są m.in. podczas:

- remontów infrastruktury,
- rozbudowy węzłów komunikacyjnych,
- modernizacji torowisk i dworców,
- budowy nowych odcinków dróg i tras kolejowych,
- zabezpieczania zapleczy technicznych,
- ochrony parkingów „Park & Ride”,
- czasowej organizacji ruchu podczas wydarzeń lub objazdów.

Największą zaletą tych rozwiązań jest możliwość bardzo szybkiego wdrożenia bez konieczności prowadzenia kosztownych prac instalacyjnych. Kompletny system nadzoru może zostać uruchomiony w ciągu kilku godzin – wraz z monitoringiem, oświetleniem, transmisją danych i autonomicznym zasilaniem.

Widoczna obecność kamer działa również prewencyjnie, ograniczając ryzyko wandalizmu, kradzieży materiałów budowlanych czy nieuprawnionego dostępu do stref technicznych. Integracja z miejskimi systemami bezpieczeństwa i inteligentną

Ilustracje: Marta Kołodziejak / A&S AI Studio

infrastrukturą transportową umożliwia natomiast centralne zarządzanie zdarzeniami oraz skuteczniejszą koordynację działań służb technicznych i porządkowych.

Bezpieczeństwo miejskie i imprezy masowe

Mobilne systemy monitoringu coraz częściej stają się integralnym elementem zabezpieczania przestrzeni publicznej oraz wydarzeń masowych. Miasta i organizatorzy wydarzeń wykorzystują je wszędzie tam, gdzie konieczne jest szybkie uruchomienie skutecznego nadzoru bez rozbudowy stałej infrastruktury.

Rozwiązania tego typu znajdują zastosowanie m.in. podczas:

- koncertów i festiwali plenerowych,
- wydarzeń sportowych,
- zgromadzeń publicznych,
- jarmarków i imprez sezonowych,
- zabezpieczania stref kibica,
- reorganizacji ruchu w centrach miast,
- ochrony parkingów i zapleczy technicznych wydarzeń.

Mobilne punkty obserwacyjne wspierają kontrolę przepływu uczestników, identyfikację zagrożeń oraz nadzór nad strefami o podwyższonym ryzyku. Dzięki transmisji obrazu w czasie rzeczywistym operatorzy mogą skuteczniej koordynować działania służb porządkowych i szybciej reagować na sytuacje kryzysowe.

Coraz większe znaczenie mają także funkcje inteligentnej analizy obrazu, umożliwiające automatyczne wykrywanie pozostawionych przedmiotów, wtargnięć do stref technicznych czy nietypowych zachowań uczestników wydarzeń. Integracja monitoringu z systemami smart city oraz miejskimi centrami zarządzania kryzysowego zwiększa skuteczność ochrony i poprawia bezpieczeństwo mieszkańców.

Od ochrony do inteligentnego zarządzania bezpieczeństwem

Rosnąca wartość rynku mobilnego monitoringu jasno pokazuje, że przyszłość branży security należy do rozwiązań mobilnych, inteligentnych i samowystarczalnych. Mobilne wieże monitoringu doskonale wpisują się w ten kierunek, łącząc bezpieczeństwo fizyczne, analitykę danych oraz optymalizację kosztów operacyjnych.

Dla wielu organizacji stanowią dziś nie tylko narzędzie ochrony, ale również pierwszy krok w kierunku nowoczesnego, skalowalnego modelu zarządzania bezpieczeństwem. Umożliwiają szybkie zabezpieczenie obiektu, elastyczne dostosowanie poziomu ochrony do aktualnych potrzeb oraz efektywne zarządzanie zasobami.

W najbliższych latach mobilne systemy monitoringu będą coraz częściej pełnić funkcję inteligentnych, autonomicznych węzłów bezpieczeństwa – zintegrowanych z analityką AI, systemami smart city i zdalnym zarządzaniem operacyjnym. Dla wielu przedsiębiorstw i instytucji staną się nie dodatkiem do ochrony, lecz także centralnym elementem strategii bezpieczeństwa i ciągłości działania. •

Redakcja „a&s Polska"

PREZENTACJE MOBILNYCH WIEŻ MONITORINGU

BCS

Mini Tower – autonomiczny system ochrony nowej generacji

Mini Tower to nowoczesny, mobilny punkt ochrony przeznaczony do zabezpieczania placów budowy, parkingów, składów materiałów, obiektów tymczasowych, terenów przemysłowych oraz wydarzeń plenerowych.
Wieża na straży – Ty na plaży.

System został zaprojektowany z myślą o szybkim wdrożeniu i pracy bez konieczności tworzenia rozbudowanej infrastruktury kablowej. Dzięki całkowicie bezprzewodowej architekturze urządzenie można ustawić praktycznie w dowolnym miejscu i uruchomić w bardzo krótkim czasie.

Rozwiązanie dostępne jest w dwóch wariantach opartych na technologiach bezprzewodowych. Obie platformy obsługują do 150 urządzeń oraz 32 strefy, zapewniając stabilną komunikację dzięki obsłudze LAN, Wi-Fi oraz LTE z funkcją dual SIM.

Mini Tower wykorzystuje zaawansowane czujki z wbudowanymi kamerami, które skutecznie ograniczają liczbę fałszywych alarmów. Zasięg detekcji do 15 metrów przy kącie 90° pozwala efektywnie chronić teren wokół urządzenia. Wbudowane kamery umożliwiają natychmiastową weryfikację alarmu zarówno w dzień, jak i w nocy dzięki oświetlaczowi IR.

W przypadku wykrycia intruza system automatycznie wysyła alarm wraz ze zdjęciami do operatora lub centrum monitoringu. Dodatkowo uruchamiana jest syrena alarmowa o mocy do 105 dB oraz sygnalizacja świetlna LED, skutecznie odstraszająca niepożądane osoby. System ma również zabezpieczenie antysabotażowe chroniące urządzenie przed próbą otwarcia.

Mini Tower wyposażony jest w autonomiczne zasilanie oparte na akumulatorze żelowym 33 Ah oraz panelu solarnym 30 W, bazującym na podzespołach Victron, co umożliwia pracę bez stałego źródła energii nawet w trudnych warunkach terenowych.

Opcjonalny nadajnik Pulson LE-910 umożliwia monitoring GPS oraz telemetrykę urządzeń. W standardzie dostępna jest indywidualna okleina z logotypami klienta. Opcjonalnie można dokupić ładowarkę do słupków, ułatwiającą szybkie ładowanie systemu podczas serwisu lub instalacji. •

Więcej na: www.bcs.pl

LIVEYE

Monitoring wideo LivEye® FALCON do samodzielnej instalacji

Kompaktowy system monitoringu wideo z indywidualnym wyposażeniem do ochrony Twojej budowy, nieruchomości lub terenu zakładu z możliwością usługi Smart by Day do monitorowania postępu prac oraz rejestracji wjazdu/wyjazdu pojazdów to właśnie LivEye FALCON.

Może być używany tymczasowo lub na stałe. Umożliwia niezależne uruchamianie i pozycjonowanie. Nie jest konieczna ingerencja w infrastrukturę sieciową klienta.

LivEye FALCON to bardzo kompaktowy system monitoringu wizyjnego. Zintegrowany z obudową uchwyt do montażu na słupie umożliwia prostą i bezpieczną instalację. Lokalizację systemu można zmieniać niezależnie i dostosowywać do potrzeb. Montaż na ścianach lub masztach oznacza, że nie ma zakłóceń w ruchu drogowym lub na parkingach. Podczas pracy LivEye FALCON jest

w bezpośrednim kontakcie z centrum monitorowania alarmów. W przypadku wykrycia alarmu intruzi mogą – w zależności od wcześniejszych ustaleń – zostać powiadomieni przez głośnik zintegrowany z systemem lub odstraszeni przez syrenę. LivEye FALCON nie jest zależny od żadnej innej infrastruktury sieciowej, a zatem nie ma problemów z wytycznymi bezpieczeństwa IT klienta.

Zalety LivEye FALCON:

- Łatwa instalacja dzięki zintegrowanemu uchwytowi na obudowie lub wspornikowi ściennemu
- Kompaktowe wymiary
- Zasilanie po stronie klienta poprzez złącze 230V
- Dodatkowy akumulator o czasie pracy do 8 godzin
- Dwie kamery bispektralne typu bullet
- Zasięg monitorowania do 180° w odległości 40 m
- 1x PTZ do śledzenia wizualnego
- Stały kontakt z centrum monitorowania
- Głośnik do zwracania się do przestępców
- Brak konieczności ingerencji w infrastrukturę sieciową klienta.

Skontaktuj się z nami i poproś o ofertę na www.liveye.pl

VCS

iTower™ Observa by VCS

iTower™ Observa by VCS to najnowszy model mobilnej wieży monitoringowej w ofercie marki VCS, stworzony z myślą o użytkownikach oczekujących kompaktowego rozwiązania bez kompromisów w zakresie funkcjonalności i możliwości technologicznych.

Konstrukcja została opracowana tak, aby zapewnić maksymalną mobilność, szybkie wdrożenie oraz niezawodne działanie nawet w wymagających warunkach terenowych. Dzięki połączeniu niewielkich gabarytów z rozbudowanym wyposażeniem systemowym iTower™ Observa znajduje zastosowanie wszędzie tam, gdzie konieczny jest skuteczny monitoring tymczasowy lub stały.

Wieża doskonale sprawdza się m.in. przy czasowej kontroli prędkości, monitorowaniu peronów kolejowych, przejść dla pieszych, parkingów, parków miejskich, hal garażowych, placów budowy czy terenów zagrożonych nielegalnym składowaniem odpadów. Może być także wykorzystywana podczas wydarzeń masowych oraz do ochrony infrastruktury krytycznej.

Jednym z największych atutów wieży iTower™ Observa jest jej kompaktowa konstrukcja, która umożliwia łatwy transport oraz szybki montaż wykonywany nawet przez jedną osobę. Maszt teleskopowy osiąga wysokość do 4,4 m, co pozwala na skuteczną obserwację rozległego obszaru. Stabilność urządzenia zapewniają cztery wysuwane podpory, dzięki którym wieża zachowuje odporność na podmuchy wiatru dochodzące do 85 km/h.

Model został wyposażony w gotowy uchwyt umożliwiający szybki montaż urządzeń monitorujących, takich jak kamery PTZ 360°. Dodatkowym elementem zwiększającym bezpieczeństwo jest prowadzenie okablowania wewnątrz teleskopowej konstrukcji, co ogranicza ryzyko uszkodzeń mechanicznych oraz aktów wandalizmu.

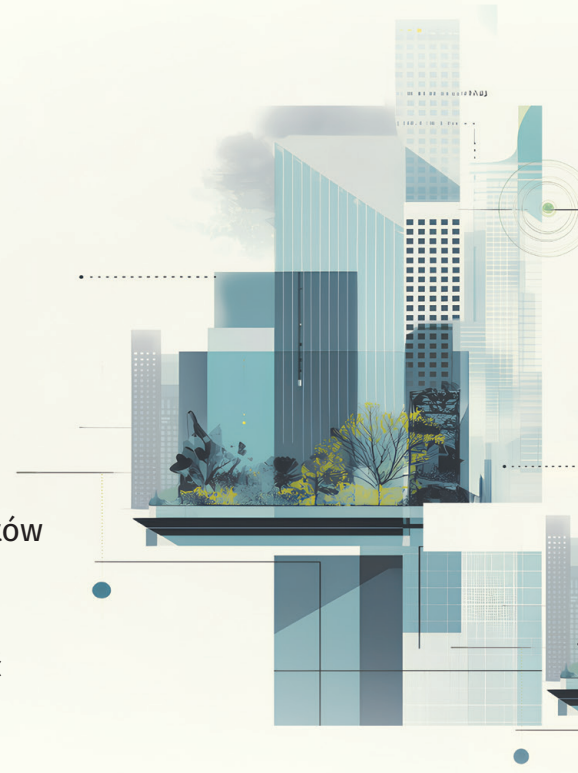
Przestronna szafa elektryczna mieści centralę komunikacyjną oraz niezbędne komponenty systemowe. Dwa uchwyty transportowe umożliwiają wygodne przemieszczanie wieży przy użyciu wózka

widłowego lub paletowego. Autonomiczność pracy zapewniają dwa demontowalne panele fotowoltaiczne o mocy 2 x 200 Wp, system zasilania awaryjnego oparty na akumulatorze i UPS oraz ogniwo paliwowe zasilane metanolem.

Oferta VCS obejmuje szerokie portfolio mobilnych rozwiązań zabezpieczających – od wież oświetleniowych po zaawansowane systemy detekcji dronów – dostosowanych do różnych zastosowań i wymagań użytkowników.

Więcej na: www.vcs.pl

Głos branży



Bezpieczeństwo w mieście to jeden z najważniejszych tematów współczesnych aglomeracji. O wyzwaniach i skutecznych rozwiązaniach rozmawiają eksperci branżowi oraz praktycy z wieloletnim doświadczeniem. Ich wiedza pozwala spojrzeć na bezpieczeństwo mieszkańców z różnych perspektyw.

Bezpieczny Wrocław

ROBERT BEDNARSKI
DYREKTOR DS. SMART CITY,
URZĘDU MIEJSKIEGO WROCŁAWIA

W obecnych realiach geopolitycznych bezpieczeństwo miast należy postrzegać znacznie szerzej niż jeszcze kilka lat temu. Dziś nie dotyczy ono wyłącznie ochrony infrastruktury krytycznej czy reagowania na zagrożenia związane z przestępczością. Współczesne miasta muszą być przygotowane również na skutki cyberataków, przeciążenia systemów miejskich, ekstremalne zjawiska pogodowe, awarie infrastruktury oraz zakłócenia w funkcjonowaniu usług publicznych. Dlatego inwestowanie w nowoczesne systemy bezpieczeństwa i budowanie odporności miejskiej stało się jednym z najważniejszych elementów odpowiedzialnego zarządzania miastem.

Kluczową rolę we współczesnym zarządzaniu miastem odgrywają dziś technologie wspierające zarówno działania operacyjne, jak i zarządzanie sytuacjami kryzysowymi. Inwestycje w nowoczesny monitoring miejski, inteligentne systemy zarządzania ruchem, centra operacyjne oraz narzędzia integrujące komunikację służb pozwalają nie tylko szybciej identyfikować potencjalne zagrożenia, ale również skuteczniej koordynować działania różnych jednostek odpowiedzialnych za bezpieczeństwo mieszkańców.

We Wrocławiu bezpieczeństwo traktujemy jako element długofalowej polityki miejskiej, obejmującej zarówno inwestycje technologiczne i infrastrukturalne, jak również działania edukacyjne i społeczne. Przykładem jest program „Bezpieczny Wrocław", którego celem jest wzmacnianie kompetencji mieszkańców w zakresie reagowania na sytuacje kryzysowe. Program obejmuje bezpłatne szkolenia, warsztaty dla mieszkańców, działania edukacyjne podczas wydarzeń miejskich oraz szkolenia online. Szczególny nacisk kładziemy na praktyczne umiejętności, takie jak pierwsza pomoc, reagowanie w sytuacjach zagrożenia czy właściwe przygotowanie do ewakuacji. Odporność miasta zaczyna się bowiem od świadomych i dobrze przygotowanych mieszkańców. •

Katowice zainwestowały w bezpieczeństwo

MACIEJ STACHURA
WICEPREZYDENT KATOWIC

W obecnych realiach geopolitycznych inwestowanie w nowoczesne systemy bezpieczeństwa przestało być elementem rozwoju miasta – stało się warunkiem jego stabilnego funkcjonowania. Dziś bezpieczeństwo nie ogranicza się już wyłącznie do porządku publicznego. Obejmuje odporność na cyberataki, skutki zmian klimatu, awarie infrastruktury krytycznej czy zdolność do reagowania na sytuacje kryzysowe, które jeszcze kilka lat temu wydawały się mało prawdopodobne. Nowoczesne miasto musi umieć przewidywać zagrożenia, a nie tylko na nie odpowiadać. Dlatego w samorządach coraz częściej inwestujemy w inteligentne systemy monitoringu, rozwiązania wspierające zarządzanie kryzysowe oraz technologie pozwalające analizować dane w czasie rzeczywistym. To właśnie informacje, szybkość reakcji i sprawna koordynacja służb stają się dziś najważniejszymi elementami bezpieczeństwa.

Jednym z filarów bezpieczeństwa w naszym mieście jest Katowicki Inteligentny System Monitoringu i Analizy (KISMiA), który liczy obecnie ponad 430 kamer. Co ciekawe, KISMiA jest zintegrowany z ITS, czyli inteligentnym systemem zarządzania ruchem, co pozwala dodatkowo wykorzystywać ponad 100 kamer. System jest inteligentny – sam wykrywa sytuacje zagrożenia i alarmuje dyspozytorów. Dzięki temu obraz z kamer jest obserwowany przez zaledwie kilku funkcjonariuszy Straży Miejskiej, co pozwala kierować większą liczbę funkcjonariuszy do pracy w terenie. KISMiA to największy w tej skali system monitoringu w Polsce. Często gościmy delegacje z innych miast, których przedstawiciele chcą wdrażać podobne rozwiązania u siebie. Z takiej wymiany doświadczeń zawsze korzystają dwie strony! KISMiA pozwala policji i straży miejskiej reagować w czasie rzeczywistym. Jednocześnie obraz z kamer był tysiące razy zabezpieczany przez policję lub prokuraturę jako materiał dowodowy.

W Katowicach konsekwentnie budujemy model odpornego miasta. Na naszym terenie funkcjonuje obecnie dziewięć czujników monitorujących poziom rzek i cieków wodnych. Rozwijamy ten system i integrujemy go z rozwiązaniami wykorzystywanymi przez spółki miejskie, aby jeszcze skuteczniej przeciwdziałać skutkom gwałtownych opadów oraz lokalnym podtopieniom. Informacje płynące z czujników, w połączeniu z siecią utworzonych w ostatnich latach zbiorników retencyjnych, pozwoliły ograniczyć lokalne podtopienia. To odpowiedź na wyzwania klimatyczne, które coraz częściej dotykają miasta w całej Europie.

Inwestycje w systemy bezpieczeństwa mają dziś znaczenie strategiczne. Decydują o ciągłości działania transportu publicznego, usług komunalnych i infrastruktury krytycznej, a także o zdolności miasta do funkcjonowania w warunkach kryzysu. Odporność staje się jednym z najważniejszych wskaźników jego nowoczesności. Miasto bezpieczne to nie tylko miasto chronione – to miasto przygotowane. Takie, które potrafi dostrzec zagrożenie odpowiednio wcześnie i skutecznie zareagować, zanim problem przerodzi się w kryzys. •

Inwestycje w systemy bezpieczeństwa

MICHAŁ KALINOWSKI
SERIS KONSALNET

Inwestycje w systemy bezpieczeństwa miasta nie powinny być postrzegane jako koszt dodatkowy, lecz jako integralny element infrastruktury miejskiej – równie istotny jak drogi, transport publiczny czy oświetlenie uliczne. Wszystkie te obszary łączy jeden wspólny mianownik: wpływają bezpośrednio na jakość życia, komfort oraz bezpieczeństwo mieszkańców.

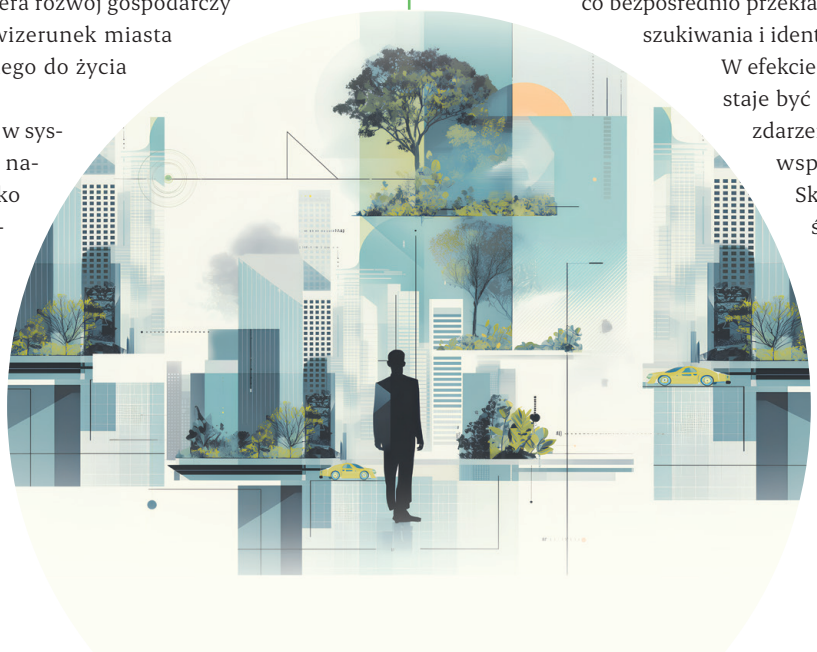
Kluczowe jest przesunięcie perspektywy z reaktywnej na prewencyjną. Nowoczesne miasta mierzą się dziś nie tylko z wyzwaniami komunikacyjnymi czy środowiskowymi, ale również z rosnącą złożonością sytuacji kryzysowych w przestrzeni publicznej. Incydenty wymagające szybkiej reakcji mogą wystąpić w każdym miejscu – na przystanku, w parku, w urzędzie czy w przestrzeni handlowej. W takich sytuacjach czas reakcji ma bezpośrednie przełożenie na zdrowie i życie ludzi.

Rozwiązania monitoringu i szybkiego powiadamiania nie zastępują infrastruktury miejskiej – one ją uzupełniają i podnoszą jej efektywność. Tak jak sygnalizacja świetlna porządkuje ruch drogowy, tak nowoczesne systemy bezpieczeństwa porządkują reakcję na zdarzenia kryzysowe.

Włodarze miejscy coraz częściej podejmują decyzje inwestycyjne w oparciu o twarde dane: statystyki interwencji, czas reakcji służb czy koszty skutków zdarzeń. W tym kontekście inwestycje w bezpieczeństwo powinny być analizowane przez pryzmat nie tylko budżetu, ale również potencjalnych oszczędności społecznych i zdrowotnych wynikających z szybszej reakcji i ograniczenia skutków incydentów.

Bezpieczeństwo jest jednym z podstawowych czynników wpływających na atrakcyjność miasta – zarówno dla mieszkańców, jak i inwestorów. Nowoczesna, dobrze zabezpieczona przestrzeń publiczna zwiększa poczucie komfortu, wspiera rozwój gospodarczy i buduje pozytywny wizerunek miasta jako miejsca przyjaznego do życia i pracy.

Dlatego inwestycje w systemy bezpieczeństwa należy traktować nie jako konkurencję dla infrastruktury miejskiej, ale jako jej naturalne i niezbędne uzupełnienie – równie strategiczne, jak rozwój transportu czy modernizacja dróg. •



Od pasywnego zapisu do aktywnej analizy obrazu

EWELINA WÓJCIK
BCS

Monitoring miejski od lat stanowi fundament systemów bezpieczeństwa. Przy obecnej skali instalacji, setkach, a często tysiącach kamer, kluczowym wyzwaniem staje się jednak nie samo rejestrowanie obrazu, ale szybkie wyszukiwanie konkretnych zdarzeń w ogromnej ilości danych wideo.

Nowoczesne rejestratory, takie jak BCS Line serii 8K-AI2 oraz -AI3/Pro, wyraźnie pokazują zmianę podejścia – od pasywnego zapisu do aktywnej analizy obrazu. System przestaje być jedynie magazynem nagrań, a zaczyna wspierać operatora w interpretacji zdarzeń i podejmowaniu decyzji.

W serii 8K-AI2 (np. BCS-L-NVR0802-A-8K-AI2) kluczową rolę odgrywa technologia AcuPick, która umożliwia wskazanie osoby lub pojazdu i automatyczne odnalezienie tego samego obiektu w obrazach z innych kamer. Dzięki analizie cech, takich jak sylwetka czy kolor ubioru, możliwe jest szybkie odtworzenie przebiegu zdarzenia i skrócenie czasu analizy.

Seria -AI3/Pro (np. BCS-L-NVR3202-A-8K-AI3/PRO) rozwija te możliwości, wprowadzając dodatkowo technologię WizSeek. Pozwala ona wyszukiwać nagrania na podstawie opisu – użytkownik wpisuje frazę, a system odnajduje odpowiadające jej zdarzenia. W praktyce oznacza to odejście od tradycyjnego przeglądania materiału na rzecz intuicyjnego wyszukiwania, które przypomina pracę z wyszukiwarką.

Warto podkreślić, że nowoczesna analiza obrazu oparta na dużych modelach AI pozwala na rozróżnianie różnych typów obiektów – ludzi, pojazdów, a także zwierząt czy nietypowych zdarzeń w przestrzeni publicznej. Przekłada się to bezpośrednio na ograniczenie liczby fałszywych alarmów i zwiększenie skuteczności systemu.

Istotnym elementem wpływającym na skuteczność AI jest jakość obrazu, szczególnie w nocy. Kamery rejestrujące obraz w kolorze dostarczają więcej informacji niż obraz czarno-biały, co bezpośrednio przekłada się na dokładność wyszukiwania i identyfikacji obiektów.

W efekcie monitoring miejski przestaje być systemem rejestrującym zdarzenia, a staje się aktywnym wsparciem dla operatorów. Skraca się czas reakcji, rośnie efektywność analizy, a dostęp do informacji jest szybszy i bardziej intuicyjny.

Sztuczna inteligencja w monitoringu nie jest już kierunkiem rozwoju – stała się standardem. •

Miejska kopuła antydronowa

ARTUR NOWAKOWSKI
Linc Polska

Współczesna ochrona obiektów infrastruktury krytycznej (IK) opiera się na koncepcji bezpieczeństwa warstwowego. Zakłada ona tworzenie wzajemnie uzupełniających się poziomów zabezpieczeń: od ochrony fizycznej (ogrodzenia, kontrola dostępu), przez systemy techniczne (monitoring, detekcja intruzów), aż po procedury organizacyjne i zarządzanie incydentami. Każda warstwa ma za zadanie opóźnić, wykryć lub uniemożliwić wystąpienie zagrożenia, a ich łączne działanie znacząco podnosi odporność danego obiektu.

Obecnie model ten wymaga jednak rozszerzenia o nowy wymiar zagrożeń – przestrzeń powietrzną, szczególnie w kontekście nieautoryzowanego wykorzystania dronów. Pojedyncze obiekty IK coraz częściej wdrażają własne systemy detekcji, jednak ich skuteczność pozostaje ograniczona zarówno zasięgiem, jak i brakiem szerszego kontekstu sytuacyjnego. W praktyce oznacza to, że ochrona warstwowa kończy się na granicy działki, podczas gdy zagrożenie może powstawać znacznie wcześniej.

Rozwiązaniem może być stworzenie miejskiej „kopuły" ochrony powietrznej – nadrzędnej warstwy bezpieczeństwa obejmującej cały obszar aglomeracji. System oparty na sieci sensorów oraz wspólnej analizie danych umożliwiałby wykrywanie, śledzenie i klasyfikację obiektów latających jeszcze przed ich dotarciem do infrastruktury strategicznej. W dalszym etapie możliwa byłaby także skoordynowana neutralizacja zagrożeń, realizowana zgodnie z obowiązującymi przepisami i przy współudziale uprawnionych służb.

Kluczową rolę w budowie takiego rozwiązania powinien odgrywać samorząd miejski pełniący funkcję integratora działań i podmiotu koordynującego współpracę. To właśnie miasto posiada unikalną możliwość łączenia interesów różnych uczestników systemu – od operatorów infrastruktury krytycznej, przez właścicieli obiektów komercyjnych, po służby publiczne. Model oparty na partnerstwie publiczno-prywatnym pozwala nie tylko rozłożyć koszty inwestycji, lecz przede wszystkim stworzyć spójny system reagowania na zagrożenia.

Wdrożenie miejskiej warstwy ochrony powietrznej leży w interesie wszystkich stron. Operatorzy infrastruktury zyskują wcześniejsze ostrzeganie i wyższy poziom bezpieczeństwa, miasto zwiększa swoją odporność na nowe zagrożenia, a mieszkańcy otrzymują realną ochronę przestrzeni, w której funkcjonują. Jest to naturalna ewolucja koncepcji bezpieczeństwa warstwowego – od poziomu pojedynczego obiektu do skali całego miasta. •

Jak zbudować cyberodporne środowisko miejskie

DANIEL KAMIŃSKI
Orange Polska

Cyberprzestępczość to dziś jedna z największych gałęzi światowego biznesu. Straty liczone są już nie w miliardach, lecz w bilionach dolarów. Wbrew powszechnemu przekonaniu ofiarami nie padają wyłącznie banki czy duże międzynarodowe korporacje. Coraz częściej atakowane są mniejsze firmy, a także samorządy, które nie zawsze dysponują zaawansowanymi mechanizmami ochrony.

Przyznaję, że jednostki samorządowe mają coraz większą świadomość zagrożeń, jednak poziom przygotowania na ewentualny atak nadal nie jest zadowalający.

I nie chodzi tu o brak pieniędzy czy niedostępność rozwiązań. Wręcz przeciwnie – dzięki projektom europejskim i innym formom dofinansowania w samorządach spotykam sprzęt oraz rozwiązania z wyższej półki. Problem polega jednak na tym, że często pozostają one w magazynach i nie są uruchamiane. Moim zdaniem powodów jest kilka.

Pierwszym jest brak wykwalifikowanej kadry IT. Informatyk pracujący „na chwilę" nie jest w stanie jednocześnie dbać o utrzymanie infrastruktury i rozwijać cyberhigieny organizacji. Drugim problemem są skomplikowane oraz zaawansowane mechanizmy zabezpieczeń, np. konfiguracja rozwiązań typu UTM – zaawansowanych routerów i zapór sieciowych – czy systemów EDR, które stale monitorują urządzenia końcowe, takie jak komputery i laptopy, oraz dostosowanie ich do specyfiki organizacji urzędu.

Rozwiązaniem, które może zmienić tę sytuację, są usługi zarządzane, w ramach których dostawca nie tylko sprzedaje rozwiązania, ale również je wdraża i utrzymuje.

Dzięki odpowiedniemu wsparciu usługodawcy IT/Cyber (ICT) nawet informatyk zatrudniony na część etatu jest w stanie zbudować cyberodporne środowisko, przygotowane na współczesne zagrożenia. •

Kamery nasobne (*body worn cameras* – BWC) stały się jednym z najważniejszych narzędzi współczesnych służb odpowiedzialnych za bezpieczeństwo publiczne. Ich wykorzystanie w policji i strażach gminnych/miejskich ma służyć nie tylko dokumentowaniu interwencji, ale również zwiększeniu transparentności działań funkcjonariuszy, poprawie jakości materiału dowodowego oraz ograniczaniu agresji wobec patroli.

Wojciech Kawa

Kamery nasobne w policji i straży miejskiej. Prawo, praktyka, przyszłość

W ostatnich latach nastąpił dynamiczny rozwój wykorzystania kamer nasobnych. Jednocześnie pojawiły się istotne problemy prawne dotyczące zakresu rejestrowania obrazu i dźwięku, ochrony prywatności oraz przetwarzania danych osobowych. Należy również zauważyć, że przepisy regulujące stosowanie kamer nasobnych w policji oraz strażach miejskich nie są jednolite i różnią się zarówno pod względem podstaw prawnych, jak i zasad rejestrowania, przechowywania oraz udostępniania nagrań.

Podstawy prawne stosowania kamer nasobnych w policji

Podstawowym aktem regulującym możliwość stosowania kamer nasobnych przez policję jest ustawa z dnia 6 kwietnia 1990 r. o Policji.

Kluczowe znaczenie mają:

- art. 15 ust. 1 pkt 5a i 5b ustawy,
- art. 15c ustawy,
- oraz przepisy wykonawcze.

Zgodnie z art. 15 ustawy policja może obserwować i rejestrować obraz zdarzeń w miejscach publicznych, obserwować i rejestrować obraz lub dźwięk podczas interwencji w miejscach innych niż publiczne, a także podczas działań kontrterrorystycznych i w policyjnych środkach transportu.

Art. 15c ustawy przewiduje obowiązek uprzedzenia osoby o rejestrowaniu obrazu lub dźwięku „w miarę możliwości".

Funkcjonariusze tej służby zostali wyposażeni w kompetencję do rejestrowania obrazu i dźwięku w przestrzeni zarówno publicznej, jak i prywatnej. W przypadku przestrzeni prywatnej uprawnienie to posiadają jednak dopiero od czasu wejścia w życie nowelizacji ustawy o Policji w lutym 2019 r. oraz obwarowane jest ono pewnymi ograniczeniami.

Szczegółowe zasady wykonywania tych uprawnień określało Rozporządzenie Rady Ministrów z dnia 4 lutego 2020 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów. Zostało ono znowelizowane poprzez Rozporządzenie

Rady Ministrów z 8 listopada 2023 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów.

Rozporządzenie reguluje m.in. sposoby rejestrowania obrazu i dźwięku, dokumentowania czynności, przechowywanie nagrań oraz zasady prowadzenia obserwacji jawnej i zdalnej.

Istotne znaczenie praktyczne mają również akty wewnętrzne Komendanta Głównego Policji, regulujące:

- organizację służby,
- wyposażenie funkcjonariuszy,
- standardy używania kamer: „Instrukcja użytkowania Systemu Rejestracji Audio-Wideo (RAW), w tym kamer nasobnych pozostających na wyposażeniu policjantów służby prewencyjnej”
- oraz procedury archiwizacji materiałów audiowizualnych.

Rozwój wykorzystania kamer nasobnych w policji

Pierwsze pilotażowe wdrożenia kamer nasobnych w policji rozpoczęły się w latach 2017–2018. Program pilotażowy prowadzono m.in. w garnizonach stołecznym, dolnośląskim oraz podlaskim. Po 2020 r. nastąpił dynamiczny rozwój systemu. Kamery są obecnie stosowane przede wszystkim przez:

- oddziały prewencji policji,
- policjantów ruchu drogowego,
- patrole interwencyjne,
- dzielnicowych,
- funkcjonariuszy zabezpieczających imprezy masowe
- oraz niektóre pododdziały kontrterrorystyczne.

Kamery nasobne mają kilka podstawowych funkcji.

- Funkcja dowodowa polega na tym, że nagrania stanowią materiał wykorzystywany w postępowaniach karnych, wykroczeniowych, dyscyplinarnych oraz administracyjnych.
- Funkcja ochronna kamer przejawia się w ograniczaniu liczby fałszywych skarg, zwiększaniu bezpieczeństwa funkcjonariuszy oraz dokumentowaniu przebiegu interwencji. Kamery pomagają również przeciwdziałać manipulacji nagraniami z telefonów komórkowych oraz ograniczają agresję wobec patroli. Ponadto budują transparentność działań służb, zwiększając zaufanie do formacji mundurowych poprzez dokumentowanie przebiegu działań i ochronę przed fałszywymi oskarżeniami o nadużycia. Świadomość nagrywania wpływa także na poprawę profesjonalizmu służb, ponieważ sprzyja bardziej profesjonalnemu zachowaniu obu stron interwencji.

- Funkcja prewencyjna kamer nasobnych polega na tym, że świadomość rejestrowania interwencji może ograniczać agresję po stronie zarówno funkcjonariuszy, jak i obywateli. Obecność kamery często „studzi emocje" i zniechęca do agresywnego zachowania wobec osób nagrywających, co redukuje liczbę napaści. Zwiększa to również poczucie bezpieczeństwa funkcjonariuszy, którzy czują się pewniej i mają większe wsparcie podczas trudnych interwencji. Kamery nasobne umożliwiają także kontrolę działań służb oraz wzmacniają bezpieczeństwo procesowe obywateli.

Kamery nasobne w strażach miejskich

Podstawowym aktem regulującym działalność straży miejskich jest ustawa z 29 sierpnia 1997 r. o strażach gminnych. Art. 11 ust. 2 ustawy przyznaje strażom prawo do: „obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych".

Dodatkowo zastosowanie ma Rozporządzenie Rady Ministrów z 16 grudnia 2009 r. w sprawie sposobu obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych przez straż gminną (miejską).

Zakres uprawnień straży miejskich jest ograniczony. W przeciwieństwie do policji straże miejskie nie mają wyraźnej podstawy do szerokiego rejestrowania dźwięku, ponieważ ustawa odnosi się przede wszystkim do obrazu oraz do miejsc publicznych. Powoduje to istotne wątpliwości interpretacyjne dotyczące nagrywania interwencji, przetwarzania danych osobowych oraz dopuszczalności rejestracji dźwięku.

W latach 2024–2026 kamery nasobne wdrożono lub testowano m.in. w Warszawie, Gdańsku, Gliwicach, we Wrocławiu, w Krakowie, Poznaniu, Rzeszowie, Bielsku-Białej oraz Szczecinie. Najczęściej korzystają z nich patrole interwencyjne, strażnicy zabezpieczający imprezy masowe, patrole nocne oraz zespoły kontroli porządku publicznego.

Problem ochrony danych osobowych

Prezes Urzędu Ochrony Danych Osobowych wielokrotnie podkreślał, że kamery nasobne stanowią formę monitoringu wymagającą:

- jednoznacznej podstawy prawnej,
- proporcjonalności,
- minimalizacji danych,
- oraz odpowiednich zabezpieczeń systemowych.

Szczególne kontrowersje budzą kwestie związane z nagrywaniem dźwięku, analizą zgromadzonych nagrań, okresem przechowywania danych oraz możliwością automatycznej identyfikacji osób.

MSWiA od kilku lat analizuje możliwość doprecyzowania przepisów ustawy o strażach gminnych tak, aby uregulować stosowanie kamer nasobnych przez strażników miejskich. Od 21 maja 2024 r. działa grupa robocza ds. straży miejskich i gminnych w ramach Komisji Wspólnej Rządu i Samorządu Terytorialnego, a wypracowane postulaty zostały skierowane do MSWiA. Na dziś widać raczej etap konsultacyjno-petycyjny niż gotową nowelizację, która precyzyjnie wpisywałaby kamery nasobne do ustawy o strażach gminnych.

Sztuczna inteligencja i przyszłość kamer nasobnych

Rozwój kamer nasobnych coraz częściej opiera się na wykorzystaniu sztucznej inteligencji. Nowoczesne systemy integrują analizę obrazu i dźwięku, automatyczną transkrypcję interwencji, rozpoznawanie twarzy, analizę zachowań agresywnych czy wykrywanie broni. Technologie te są rozwijane m.in. w USA i Wielkiej Brytanii i mają zwiększać bezpieczeństwo funkcjonariuszy, przyspieszać reakcję służb oraz usprawniać analizę materiału dowodowego.

Istotnym kierunkiem rozwoju jest przesyłanie obrazu i dźwięku w czasie rzeczywistym do stanowisk kierowania. Pozwala to lepiej zarządzać interwencjami i wspierać funkcjonariuszy w sytuacjach kryzysowych, np. przy utracie kontaktu. Coraz większą rolę będą odgrywać również usługi chmurowe, które ułatwią przechowywanie, analizę i udostępnianie nagrań.

Sztuczna inteligencja ma automatyzować procesy analityczne, ograniczać czas pracy związanej z przetwarzaniem danych oraz umożliwiać tworzenie bardziej precyzyjnych raportów. W przyszłości możliwe stanie się także profilowanie zachowań sprawców w czasie rzeczywistym. Jednocześnie rozwój tych technologii wymaga zachowania równowagi między bezpieczeństwem publicznym a ochroną praw obywatelskich i danych osobowych.

Nowe możliwości oznaczają także nowe zagrożenia. Należą do nich masowa analiza danych, profilowanie obywateli, błędy algorytmiczne oraz wzrost poziomu nadzoru państwa, mogący ograniczać prywatność i swobody obywatelskie.

Podsumowanie

Kamery nasobne stały się trwałym elementem funkcjonowania służb publicznych w Polsce. W policji ich stosowanie posiada stosunkowo silne podstawy prawne i rozwijający się system organizacyjny. W strażach miejskich regulacje pozostają mniej precyzyjne, szczególnie w zakresie rejestrowania dźwięku.

Technologie te stają się także częścią koncepcji inteligentnych miast (smart cities), wspierając systemy bezpieczeństwa publicznego i zarządzania danymi. W najbliższych latach kluczowe będzie doprecyzowanie przepisów, stworzenie jednolitych standardów użycia oraz uregulowanie wykorzystania AI.

Kamery nasobne nie zastąpią profesjonalizmu funkcjonariuszy, ale mogą zwiększać transparentność działań służb, poprawiać jakość materiału dowodowego i podnosić poziom bezpieczeństwa. Największym wyzwaniem pozostanie jednak odpowiedź na pytania dotyczące analizy, przechowywania i kontroli danych oraz granicy między bezpieczeństwem publicznym a cyfrowym nadzorem państwa. •

Wojciech Kawa
Młodszy inspektor policji w stanie spoczynku, były zastępca Komendanta Miejskiego Policji w Poznaniu ds. Kryminalnych.

Ilustracje: Marta Kołodziejak / A&S AI Studio

Kamery nasobne w branży ochrony – problem technologiczny czy prawny?

W dobie cyfryzacji, AI, dronów i systemów antydronowych kamery nasobne nie wydają się niczym nowym ani kontrowersyjnym. Przywykliśmy do zapisów interwencji policji, w których obok obrazu utrwalana jest również ścieżka audio. Dlaczego więc nie są one powszechnym wyposażeniem pracowników ochrony – nie tylko grup interwencyjnych, lecz także osób pracujących w centrach handlowych, sklepach, przy obsłudze bankomatów czy dostawach do magazynów?

Krzysztof Chylarecki

Koszt zakupu kamery nasobnej jest niski – od kilkudziesięciu do kilkuset złotych. Procedury używania i archiwizowania nagrań oraz administrowania nimi również nie wydają się barierą nie do pokonania. Problem nie leży więc ani w technologii, ani w kosztach.

Przepisy branżowe nie przyznają pracownikom ochrony uprawnienia do utrwalania obrazu i dźwięku z wykonywanych zadań w sposób analogiczny do uprawnień funkcjonariuszy policji. Zdroworozsądkowo można jednak uznać, że zapis audio-wideo z interwencji nie musi godzić w dobra osób, wobec których podejmowane są czynności, lecz może wręcz je chronić. Pracownik ochrony sporządza notatkę z interwencji, opisując jej przebieg, w tym zachowanie osoby ujętej. Nagranie pozwalałoby zweryfikować zgodność takiej notatki ze stanem faktycznym.

Skoro urządzenie jest tanie, procedury możliwe do wdrożenia, a wartość dowodowa oczywista, dlaczego rozwiązanie to nie przyjęło się powszechnie? Ze stanowiska MSWiA DZIK-IV.6610.5.7.2023 nie wynika ani jednoznaczny zakaz, ani wyraźne przyzwolenie na stosowanie kamer nasobnych przez agencje ochrony. Wniosek praktyczny jest jednak czytelny: problem nie ma charakteru operacyjnego czy finansowego, lecz prawny.

Na gruncie RODO dopuszczalność takiego rozwiązania wymagałaby istnienia podstawy przetwarzania z art. 6 ust. 1 RODO oraz przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 RODO. UODO w stanowisku DOL.23.261.2023.WL.OJ uznał monitoring nasobny za formę wysoce inwazyjną, a przez to nadmiarową jako element wyposażenia pracowników ochrony. W ocenie UODO rozwiązanie to naruszałoby zasadę minimalizacji danych, czyli wymóg adekwatności oraz ograniczenia zakresu danych do tego, co niezbędne dla celu przetwarzania.

Po głębszym namyśle można uznać, że stanowisko to ma swoje uzasadnienie. Kamery nasobne nie są jedynym środkiem technicznym, który można uznać za nadmiarowy względem celu ochrony. Podobnie można oceniać sygnały świetlne i dźwiękowe na pojazdach ochrony, kajdanki używane prewencyjnie, podsłuch czy przeszukiwanie osób i rzeczy.

W innych państwach UE problem również istnieje. Kraje rozwiązują go w różny sposób – od całkowitego zakazu po warunkowe dopuszczenie w jasno określonych granicach, bez dostępu osoby rejestrującej do nagrań. Szczególne znaczenie ma tu obowiązek informacyjny. W wyroku TSUE z 18 grudnia 2025 r. w sprawie C-422/24 uznano, że przy zbieraniu danych za pomocą kamery nasobnej zastosowanie ma art. 13, a nie art. 14 RODO. Dane są bowiem zbierane bezpośrednio od osoby nagrywanej, dlatego informacja o przetwarzaniu powinna być dostępna już na etapie pozyskiwania danych.

Orzeczenie TSUE nie oznacza jednak, że pracownicy ochrony mogą swobodnie używać kamer nasobnych. Przesądza jedynie, że obowiązek informacyjny powinien być realizowany w chwili zbierania danych, a nie później.

Dlatego wniosek dla polskiej branży ochrony jest mniej otwarty, niż mogłoby się wydawać. Przy obecnym stanowisku UODO kamery nasobne z zapisem obrazu i dźwięku nie stanowią bezpiecznego rozwinięcia monitoringu ani zwykłego elementu wyposażenia pracownika ochrony. Do czasu pojawienia się wyraźnej podstawy prawnej określającej cel, sytuacje użycia, zasady dostępu do nagrań, okres retencji oraz odpowiedzialność administratora ich stosowanie pozostaje obarczone ryzykiem działania wbrew stanowisku organu nadzorczego. •

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

ALNET SYSTEMS

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

www.alnetsystems.com

Kto i dla kogo opracował normę PN-EN 62676 „Systemy dozoru wizyjnego”

Wieloczęściową normę PN-EN 62676 opracowaliśmy sami dla siebie – producenci, projektanci i użytkownicy systemów dozoru wizyjnego dla producentów, projektantów i użytkowników systemów dozoru wizyjnego. W drugim wydaniu części IEC 62676-4:2025-10 na nowo zdefiniowaliśmy zadania operatora (cele prowadzenia dozoru wizyjnego). Nowym zadaniom nadaliśmy nowe nazwy – określone w normie skrótem O2DCPVS – i przypisaliśmy do nich odmienne wymagania dotyczące jakości obrazu, które oficjalnie nazwaliśmy gęstościami pikselowymi.

Waldemar Więckowski

Zadania operatora – cele obserwacji

Dlaczego MDORII zastąpiliśmy O2DCPVS?

Dlaczego zadania operatora: *Monitor, Detect, Observe, Recognise, Identify* i *Inspect* zastąpiliśmy zadaniami: *Overview, Outline, Discern, Perceive, Characterise, Validate* i *Scrutinise*? I dlaczego zadaniem podstawowym jakim dotychczas było Idenify jest teraz Scrutinise?

W informacji prasowej podpisanej przez kierownika grupy projektowej, która opracowała drugie wydanie normy, znajdują się dwa fragmenty, które można uznać za uzasadnienie tych zmian. Oba odnoszą się do podstawowego zadania operatora, jakim w systemach dozoru wizyjnego stosowanych w zabezpieczeniach jest Identyfikacja:

- „Identyfikację zdefiniowano jako «cel funkcjonalny kamery wyznaczony dla umożliwienia identyfikacji osoby ponad wszelką uzasadnioną wątpliwość». Według czołowych ekspertów kryminalistycznych ds. obrazu w organach ścigania «identyfikacja osoby ponad wszelką uzasadnioną wątpliwość» jest po prostu niemożliwa. Nawet z próbką DNA – która jest oczywiście czymś znacznie więcej niż zapisem wizyjnym – identyfikacja w 100% pozbawiona wątpliwości jest nieosiągalna”.
- „Kadr osoby zajmującej 100% wysokości ekranu dla celu identyfikacji twarzy był kwestionowany, zwłaszcza w słabym oświetleniu, przy zaszumionym obrazie i dodatkowych artefaktach kompresji, które nie były uwzględnione podczas opracowywania norm analogowych”.

Jak widać, zakwestionowano równocześnie zarówno nazwę zadania Identyfikacja, jak i przypisaną do niego w normie z 2014 r. jakość obrazu.

O zastrzeżeniach wobec nazwy napisał także jeden z uczestników prac nad drugim wydaniem normy:

Jednym z zastrzeżeń jurysdykcji nieanglojęzycznych (non-English speaking jurisdictions) jest faktyczne znaczenie Identification w terminologii prawnej. Niektórzy argumentowali, że jedynie testy DNA umożliwiają pozytywną identyfikację osoby.

Więcej informacji dotyczących uzasadnienia przedmiotowych zmian nie udało mi się znaleźć w materiałach publicznie udostępnionych przez osoby związane z opracowaniem normy.

Normatywny termin „Identyfikacja”

Przyjmując, że powyższe cytaty oddają istotę dyskusji prowadzonej w IEC o potrzebie zmiany nazw zadań operatora systemu dozoru wizyjnego, wychodzi na to, że co najmniej mylone było w niej słowo „Identyfikacja” z terminem „Identyfikacja”.

Różnica – w uproszczeniu – polega na tym, że słowo (bądź określony zestaw słów) staje się w normie terminem wtedy, gdy zostanie w niej zdefiniowane jego znaczenie w zakresie stosowania tej normy. Identyfikacja jest w normie IEC 62676-4:2014-04 terminem, a nie słowem, i dotyczy wyłącznie zadania operatora w systemach dozoru wizyjnego stosowanych w zabezpieczeniach.

W normalizacji obowiązuje zasada, że termin zdefiniowany w normie oznacza to i tylko to, co stanowi jego definicja zamieszczona w tej normie. Co równie ważne, znaczenie to odnosi się wyłącznie do zakresu stosowania danej normy.

Innymi słowy, termin Identyfikacja w znaczeniu określonym w normie IEC 62676-4:2014-04 odnosi się wyłącznie do zadania operatora systemów dozoru wizyjnego stosowanych w zabezpieczeniach. W żadnym przypadku określony w tej normie termin Identyfikacja nie powinien być stosowany w odniesieniu do zapisów innych norm, w których występuje słowo „Identyfikacja” – chyba że z kontekstu jednoznacznie wynika, iż chodzi o systemy dozoru wizyjnego określone w normie IEC 62676-4:2014-04.

Analogiczna zasada dotycząca znaczenia terminów i zakresu ich stosowania funkcjonuje w prawie od czasu, gdy zaczęło ono powstawać – na długo przed opracowywaniem norm. (Przepraszam za to banalne zdanie).

Jest pewne, że termin „Identyfikacja” występuje w różnych zapisach legislacyjnych. Oznacza jednak wyłącznie to, co określono w definicji zawartej w danym akcie prawnym (ustawie, rozporządzeniu) i odnosi się wyłącznie do zakresu stosowania tego prawa.

Nie należy też zapominać, że czym innym jest prawo, a czym innym normy. Normy nie są przepisami prawa, a ich stosowanie jest dobrowolne.

Zadania operatora a testy

Identyfikacja osoby w systemach dozoru wizyjnego stosowanych w zabezpieczeniach jest dokonywana przez operatora na podstawie obrazu tej osoby wyświetlanego na ekranie monitora.

W normie z 2014 r. precyzyjnie określono jakość obrazu (powszechnie, ale niepoprawnie, nazywaną gęstością pikselową) wymaganą do realizacji tego zadania. Przedstawiono także test sprawdzający, czy VSS tę jakość zapewnia.

Co ważne, w teście tym sprawdzany jest cały tor transmisyjny obrazu sceny – poczynając od obiektywu kamery, a kończąc na wyświetlaczu monitora. Test przeprowadza się z użyciem planszy testowej rozdzielczości i zasadniczo nie wymaga on udziału operatora – może go wykonać każdy, kto wie, jak to zrobić.

(Odrębną kwestią jest to, w ilu zrealizowanych instalacjach VSS test ten jest faktycznie wykonywany).

O ile o normatywnym teście jakości obrazu sporadycznie wspomina się w branżowej narracji, o tyle o kolejnych dwóch testach przedstawionych w normie praktycznie zapomniano.

Oba należy przeprowadzać z udziałem operatora, aby upewnić się, że system rzeczywiście pozwala mu zrealizować zadanie Identyfikacji. W obu przypadkach operatorowi prezentuje się różne obiekty testowe w scenie wyświetlanej na ekranie monitora.

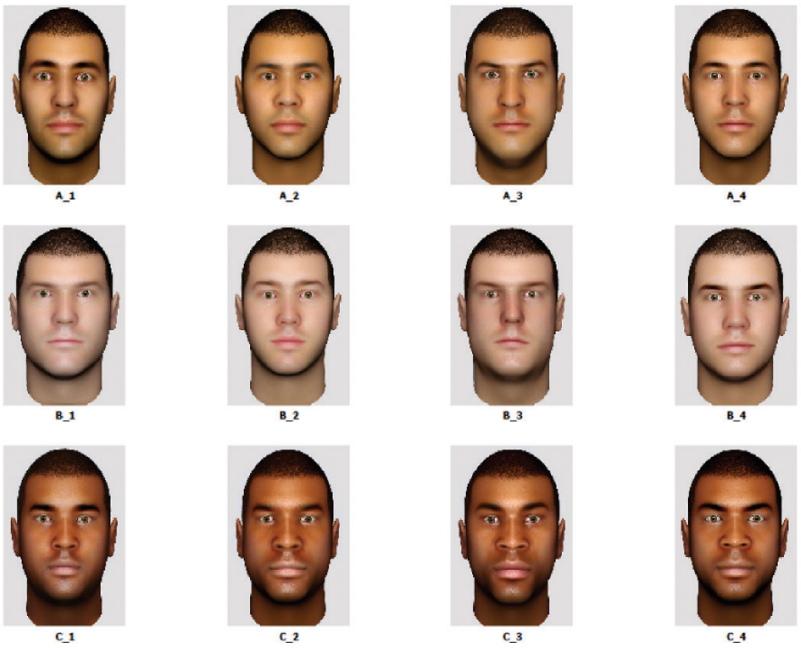
Celem pierwszego testu jest sprawdzenie możliwości wykrycia intruza w dozorowanej scenie. De facto jest to także test całego systemu, ponieważ może się zdarzyć, że system – mimo wymaganej rozdzielczości – nie umożliwia operatorowi wykrycia intruza w całej scenie i w każdych przewidywanych warunkach oświetleniowych.

Jeśli problem nie leży po stronie operatora, konieczna może być zmiana posadowienia punktów kamerowych, ich wymiana i/lub doświetlenie sceny.

Drugim testem operatora opisanym w pierwszym wydaniu normy (IEC 62676-4:2014-04) jest test identyfikacji twarzy. Wykonuje się go kilkukrotnie z użyciem dwóch losowo wybieranych plansz testowych ze zbioru przedstawionego na rysunku. (Test ten został po raz pierwszy opisany w normie EN 50132-7:2012-08 z 2012 r.).

Test o identycznej procedurze znajduje się także w najnowszym, drugim wydaniu normy IEC 62676-4:2025-10. W pierwszym wydaniu normy IEC był to test potwierdzający spełnienie kryterium zadania Identyfikacja (gęstość pikselowa wymaganego obrazu: 250 pikseli/m), natomiast w drugim jest to test zadania *Scrutinise* (1500 pikseli/m).

Ilustracje: Marta Kołodziejak / A&S AI Studio



Rys. Plansze stosowane w teście identyfikacji twarzy

Autorzy aktualnego wydania normy nie sprawdzili jednak, co znajduje się pod linkiem do strony UK Home Office, który zamieścili jako odsyłacz do miejsca pobrania plansz testowych twarzy. Plansze zostały bowiem zaktualizowane już w 2016 r. (sic!) i zawierają obrazy dwunastu, a nie dziewięciu twarzy, jak pokazano w normie. Tak było jedynie w czasie publikacji pierwszego wydania normy.

Świadczyłoby to o tym, że nikt – a przynajmniej autorzy drugiego wydania normy IEC – nie wykonuje tego testu. To mogłoby tłumaczyć powszechne przypadki, w których zapis wizyjny zdarzenia nie pozwala zidentyfikować sprawcy.

Na marginesie zagadnienia wykonywania testów systemu dozoru wizyjnego warto przywołać sentencję zamieszczoną w poradniku wydanym przez brytyjską policję w 1996 r.:

Who should be the first to test your system – you or the criminal?

(Kto pierwszy powinien przetestować twój system – ty czy przestępca?)

Wnioski: co konkretnie zmienia się w zakresie celów obserwacji?

Nowe wydanie normy PN-EN / IEC 62676-4:2025 zmienia przede wszystkim sposób definiowania celów obserwacji oraz wymaganej jakości obrazu potrzebnej do realizacji tych celów.

Dotychczasowych sześć zadań typu DORI/MDORII *(Monitor, Detect, Observe, Recognise, Identify, Inspect)* upgradowano do siedmiu nowych zadań O2DCPVS:

- ***Overview,***
- ***Outline,***
- ***Discern,***
- ***Perceive,***
- ***Characterise,***
- ***Validate,***
- ***Scrutinise.***

W praktyce oznacza to:

- rozróżnienie pomiędzy obserwacją obiektów ogólną (LPDO) a szczegółową (HPDO),
- znaczne podwyższenie wymagań jakościowych obrazu dla zadań związanych z rozpoznaniem *(Validate)* i identyfikacją *(Scrutinise)* osoby.

Najbardziej odczuwalna zmiana dotyczy dawnego zadania *Identify*. W poprzedniej wersji normy do tego zadania była przypisana jakość obrazu 250 pikseli/m. W nowym wydaniu tę rolę przejęło zadanie *Scrutinise*, wymagające 1500 pikseli/m.

Nowa norma wprowadza *bardziej realistyczne minimalne gęstości pikselowe uwzględniające różne czynniki wpływające na współczesne kamery IP, takie jak kompresja i szum.*

Nowa norma zwraca także uwagę na fakt, że wielkość obiektu na ekranie wyświetlacza powinna mieć związek z zadaniami operatora. W tym kontekście wyjaśnia dlaczego najlepszą jakość obrazu otrzymuje się wtedy, kiedy liczba pikseli wyświetlacza jest równa liczbie pikseli obrazu z kamery.

Zmiana terminologii ma także znaczenie formalne. Nowe nazwy zadań – w intencji autorów normy – mają ograniczyć ryzyko błędnej interpretacji pojęcia „identyfikacja" w kontekście prawnym i dowodowym.

W dalszej części artykułu dostępnej na naszym portalu aspolska.pl przedstawimy też odpowiedzi na pytania:

- dlaczego dawne określenie CCTV zostało zastąpione terminem VSS,
- czy rzeczywiście nowa terminologia O2DCPVS została opracowana w oparciu o normy ISO/IEC 19794-5 oraz ISO/IEC 29794-5,
- oraz dlaczego dotychczasowe terminy MDORII zastąpiono terminami O2DCPVS.

Omówimy również zależności pomiędzy nowymi zadaniami operatora, biometrią twarzy, oceną jakości obrazu oraz wymaganiami współczesnych systemów dozoru wizyjnego stosowanych w zabezpieczeniach. •

Waldemar Więckowski
Zastępca przewodniczącego Komitetu Technicznego nr 52 ds. Systemów Alarmowych Włamania i Napadu przy PKN. Wykładowca na kursach Ośrodka Szkoleniowego Polskiej Izby Systemów Alarmowych.

Krajobraz cyberzagrożeń 2025 wg CERT Orange Polska

Jak wynika z najnowszego raportu CERT Orange Polska*, główne kategorie ataków i ich udział wśród zagrożeń utrzymują się od kilku lat na podobnym poziomie. Największą część stanowi phishing – ponad 47% w 2025 roku. Kolejne miejsca zajmują ataki DDoS (niemal 16%) oraz złośliwe oprogramowanie (ponad 13%). Charakter zagrożeń i sposób realizacji ataków zmieniają się jednak diametralnie. Widać wpływ technologii, zwłaszcza AI, oraz profesjonalizację przestępczego biznesu.

* https://cert.orange.pl/ostrzezenia/raport-cert-orange-polska-2025/

W kategorii phishingu – wyłudzania danych lub pieniędzy – dominowały fałszywe inwestycje (niemal 70% wszystkich oszustw wobec zaledwie 28% dwa lata wcześniej). Coraz więcej fałszywych SMS-ów wysyłanych jest za pomocą specjalnych aplikacji. To zautomatyzowany proceder, pozwalający działać na masową skalę.

DDoS – nowe rekordy, potężne botnety

Wśród ataków DDoS największą część stanowią te krótkie, trwające poniżej 10 minut i o niskim poziomie nasilenia. W ubiegłym roku w sieci Orange zarejestrowano i zneutralizowano jednak także ataki o rekordowej sile, sięgającej nawet 1,5 Tb/s. Rok 2025 przyniósł nowe, potężne, wielomilionowe botnety umożliwiające przeprowadzanie gigantycznych ataków, takich jak np. Aisuru.

Ataki przestają być jednorazowym zdarzeniem, a zaczynają wspierać inne działania, takie jak kampanie dezinformacyjne, próby wymuszeń czy odwracanie uwagi od równolegle prowadzonych operacji. Platformizacja sprawia, że DDoS staje się łatwo dostępną „usługą", możliwą do precyzyjnego zaplanowania, co fundamentalnie zmienia jego rolę w ekosystemie zagrożeń.

Jak wskazują eksperci CERT Orange Polska, DDoS staje się dziś zagadnieniem odporności całej architektury sieciowej. Skuteczna obrona wymaga nie tylko dużych zasobów sieciowych, ale także m.in. ścisłej współpracy pomiędzy operatorami, CERT-ami i globalnymi dostawcami usług bezpieczeństwa.

Czego uczą nas ataki na infrastrukturę krytyczną i przemysłową?

Rok 2025 przyniósł dużą liczbę incydentów dotyczących technologii operacyjnych (OT) w infrastrukturze krytycznej i przemysłowej. Przeglądy bezpieczeństwa, wskazanie obszarów wymagających poprawy, zrozumienie ryzyk związanych z lukami w zabezpieczeniach oraz zdefiniowanie planu naprawczego to pierwsze kroki na drodze do budowania cyberodporności firmy.

– *W budowaniu świadomości zagrożeń i sposobów ochrony nic nie działa tak dobrze jak praktyka. W tym celu powstało nasze Laboratorium OT, gdzie pokazujemy przykłady ataków na infrastrukturę przemysłową i działanie narzędzi bezpieczeństwa. To także bezpieczne środowisko z rzeczywistymi, fizycznymi elementami automatyki i SCADA, które pozwala testować różne rozwiązania* – powiedział Krzysztof Bronarski z zespołu ICT Orange Polska.

Podobnie jak w przypadku indywidualnych użytkowników, również w firmach najważniejszym elementem systemu bezpieczeństwa są ludzie – ich świadomość i odporność na socjotechnikę. Oprócz Centrum Doświadczeń Cyberbezpieczeństwa, w którym uczymy, jak lepiej chronić firmę przed cyberatakami, budowanie świadomości wspiera także Cyber Pakiet. Oferuje on nie tylko rozwiązania, takie jak skanowanie podatności infrastruktury klienta, ochrona reputacji firmy czy informacje o wyciekach danych, ale również testy socjotechniczne, czyli uzgodnione, symulowane ataki phishingowe.

Nowym rozwiązaniem jest CyberTarcza Go, która blokuje próby wejścia na niebezpieczne strony i zapewnia bezpieczeństwo również za granicą oraz podczas korzystania z sieci Wi-Fi. Aplikacja opiera się na wiedzy CERT Orange Polska i aktywnym rozpoznawaniu zagrożeń. Co istotne, jest dostępna dla wszystkich użytkowników urządzeń mobilnych, niezależnie od tego, czy są klientami Orange, czy korzystają z usług innych operatorów: https://cybertarczago.pl/

To przydatne rozwiązanie zarówno dla użytkowników indywidualnych, jak i niewielkich firm – w ramach jednej subskrypcji można objąć ochroną trzy urządzenia. •

Orange Polska
www.cybertarczago.pl

POLON-ALFA

CNBOP-PIB

PIERWSZY W POLSCE **CERTYFIKOWANY**

PANEL OBSŁUGI DLA STRAŻY POŻARNEJ

POSP 6000

- **PEŁNA INTEGRACJA Z SYSTEMEM SYGNALIZACJI POŻAROWEJ**
  Panel współpracuje bezpośrednio z centralą – wszystkie dane są przesyłane w czasie rzeczywistym, zapewniając aktualny obraz sytuacji.
- **NATYCHMIASTOWY DOSTĘP DO KLUCZOWYCH INFORMACJI**
  Panel instalowany w odległości maks. 5 m od wejścia głównego umożliwia szybkie podjęcie działań już od pierwszych sekund akcji ratowniczej.
- **WSPARCIE DLA WSZYSTKICH SŁUŻB RATOWNICZYCH**
  Intuicyjna obsługa i przejrzystość informacji wspierają działania zarówno straży pożarnej, jak i operatorów technicznych czy personelu ochrony.

POLON-ALFA | 85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.com

Niewidzialny system, realne ryzyko. Rozmowy o sektorze, którego nie wolno zatrzymać

Są systemy, których obecność zauważamy dopiero wtedy, gdy przestają działać. Energia należy właśnie do nich. Każdego dnia uruchamia miasta, transport, szpitale, fabryki, serwery i domy. Jest niemal niewidzialnym tłem naszej codzienności. Do momentu, gdy coś zaczyna zakłócać jej rytm. To właśnie od tej perspektywy rozpoczęła się **konferencja „Bezpieczeństwo infrastruktury krytycznej, energetycznej i OZE”.** Szybko stało się jasne, że rozmowa o energetyce nie będzie dotyczyć wyłącznie produkcji energii czy rozwoju odnawialnych źródeł.

Jeszcze kilka lat temu bezpieczeństwo energetyczne kojarzyło się głównie z ciągłością dostaw. Dziś skala zagrożeń wygląda zupełnie inaczej. Energetyka coraz wyraźniej pokazuje swoją rolę jako jeden z kluczowych filarów infrastruktury krytycznej, a zarazem staje się jednym z najbardziej atrakcyjnych celów działań hybrydowych. Skala zmian w całym sektorze dodatkowo przyspiesza.

Polska energetyka przechodzi jedną z największych transformacji w swojej historii. Z jednej strony rozwój OZE jest wymogiem regulacyjnym i kierunkiem strategicznym całej Europy. Do 2030 roku Unia Europejska zakłada ograniczenie emisji gazów cieplarnianych o co najmniej 55 proc., a neutralność klimatyczna ma zostać osiągnięta do 2050 roku.

To oznacza ogromne przyspieszenie inwestycji. Nowe farmy fotowoltaiczne i wiatrowe powstają w rozproszonych lokalizacjach, często w miejscach oddalonych od dużych ośrodków miejskich. Dane prezentowane podczas konferencji pokazały skalę tego procesu – zabezpieczeniami objęto już 228 farm wiatrowych i 536 farm fotowoltaicznych, obejmujących odpowiednio 5,8 GW i 3,1 GW mocy zainstalowanej.

I właśnie tutaj pojawia się fundamentalne pytanie: czy bezpieczeństwo rozwija się równie szybko jak sama energetyka?

Zagrożenia zaczynają się dużo wcześniej

Jedna z najważniejszych zmian w myśleniu o bezpieczeństwie dotyczy dziś przesunięcia perspektywy – z pojedynczych incydentów na cały mechanizm budowania zagrożeń.

– *Raporty bezpieczeństwa bardzo często opisują incydent. Znacznie rzadziej pokazują przygotowanie gruntu pod incydent* – mówiła **mjr dr Anna Grabowska-Siwiec, emerytowana funkcjonariuszka ABW.**

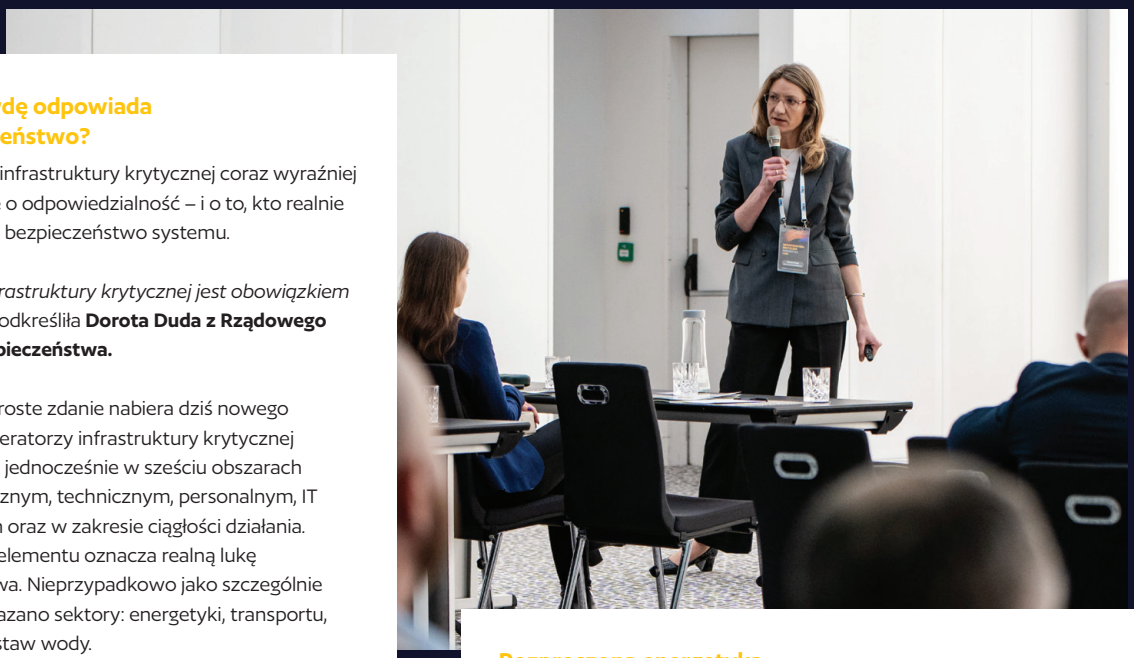
To zdanie stało się osią dyskusji. Bo współczesne zagrożenia coraz rzadziej zaczynają się od spektakularnego ataku. Najpierw pojawia się budowanie zależności technologicznych. Później wpływ na procesy decyzyjne. Następnie działania informacyjne, dezinformacja, testowanie odporności systemu. Dopiero na końcu może pojawić się sam incydent. W praktyce oznacza to, że bezpieczeństwo energetyczne przestaje być wyłącznie domeną działów IT czy ochrony fizycznej.

Gdy celem stają się procedury

Europejskie doświadczenia oraz analiza rzeczywistych incydentów pokazują, że zagrożenia dla sektora energetycznego coraz częściej przybierają mniej oczywiste formy.

– *Uszkodzenie infrastruktury nie musi być jedynym celem, ani nawet celem głównym. Rozpoznanie procedur to cel bardzo atrakcyjny, bo przenosi ryzyko na wyższy poziom* – podkreślał **Jacek Grzechowiak z Centrum Kompetencji a&s Polska.**

To szczególnie ważny wniosek dla sektora energetycznego. Coraz częściej nie chodzi już wyłącznie o fizyczne straty. Znaczenie ma także testowanie odporności organizacji, poznawanie procedur, sposobu reagowania i całego ekosystemu współpracy. Europejskie przykłady pokazują, że skala problemu obejmuje dziś zarówno sabotaże farm OZE, jak i kradzieże infrastruktury czy działania dywersyjne.



Kto naprawdę odpowiada za bezpieczeństwo?

W przypadku infrastruktury krytycznej coraz wyraźniej wraca pytanie o odpowiedzialność – i o to, kto realnie odpowiada za bezpieczeństwo systemu.

– *Ochrona infrastruktury krytycznej jest obowiązkiem operatora* – podkreśliła **Dorota Duda z Rządowego Centrum Bezpieczeństwa.**

To pozornie proste zdanie nabiera dziś nowego znaczenia. Operatorzy infrastruktury krytycznej muszą działać jednocześnie w sześciu obszarach ochrony: fizycznym, technicznym, personalnym, IT i OT, prawnym oraz w zakresie ciągłości działania. Brak jednego elementu oznacza realną lukę bezpieczeństwa. Nieprzypadkowo jako szczególnie wrażliwe wskazano sektory: energetyki, transportu, łączności i dostaw wody.

Rozproszona energetyka, rozproszone ryzyko

Rozproszenie infrastruktury odnawialnej staje się jednym z największych wyzwań współczesnej energetyki. Farmy wiatrowe i fotowoltaiczne to często obiekty oddalone od miast, rozciągnięte na dużych obszarach i wymagające zupełnie innego podejścia do ochrony niż tradycyjne instalacje.

– *Bezpieczeństwo takich obiektów zaczyna się dużo wcześniej niż na etapie montażu kamer czy systemów alarmowych. Projektowanie systemów ochrony oparte jest na analizie ryzyka dla każdej farmy oraz każdego etapu inwestycji* – mówił **Grzegorz Loose z Taurus Ochrona.**

To podejście wyraźnie pokazuje zmianę sposobu myślenia o bezpieczeństwie – od reakcji na zagrożenia do projektowania odporności już na etapie inwestycji.

W rozproszonych systemach szczególnego znaczenia nabiera również czas reakcji.

– *Bez PSIM czas reakcji na incydent wynosi od 3 do 6 minut. Z PSIM – około jednej minuty* – podkreślał **Mikołaj Kobyliński z Megavision,** pokazując rolę platform integrujących systemy bezpieczeństwa.

W świecie infrastruktury krytycznej różnica kilku minut przestaje być detalem technicznym. Może oznaczać realną różnicę między incydentem a kryzysem.

Technologia musi budować zaufanie

Wraz z rosnącą liczbą urządzeń podłączonych do sieci coraz częściej pojawia się pytanie o zaufanie do samych systemów bezpieczeństwa.

– *Ta sama kamera, którą montujesz, by poprawić bezpieczeństwo, może stać się naszym największym cyfrowym słabym punktem* – mówił **Łukasz Lik z Hanwha Vision.**

Podkreślił również, jak ważna jest idea „Secure by Design" – bezpieczeństwa projektowanego od samego początku, a nie „doklejanego" na końcu procesu. Bo zaufanie do technologii nie zaczyna się po wdrożeniu. Zaczyna się znacznie wcześniej – już na etapie projektowania.

Fałszywy alarm też kosztuje

Bezpieczeństwo to nadal połączenie elektroniki, mechaniki i człowieka.

– *Najczęściej problemy biorą się ze źle zaprojektowanej lub źle wykonanej instalacji* – podkreślał **Paweł Cendrowski z CIAS.**

To ważne przypomnienie w świecie, w którym technologia coraz częściej staje się odpowiedzią na każde zagrożenie. Bo nawet najlepsze rozwiązania nie zastąpią dobrze zaprojektowanego systemu.

Transformacja przyspiesza. Czy bezpieczeństwo nadąża?

Dynamiczny rozwój OZE przynosi także nowe wyzwania związane z cyberbezpieczeństwem.

– *Koncerny energetyczne muszą raptownie zwiększyć moc zainstalowaną ze źródeł odnawialnych* – mówił ekspert **Wojciech Kubiak.** – *Za tym przyspieszeniem idą jednak nowe problemy: brak standaryzacji, niski poziom zabezpieczeń fizycznych i koszmarnie niski poziom zabezpieczeń cybernetycznych.*

Rozproszenie infrastruktury oznacza również rozproszenie odpowiedzialności, procedur i standardów. A właśnie tam najczęściej pojawiają się luki.

Bezpieczeństwo bez kompromisów

O bezpieczeństwie nie da się dziś mówić bez kontroli dostępu. Szczególnie w środowiskach infrastruktury krytycznej, gdzie dostęp do obiektów, danych i systemów musi być jednocześnie wygodny i odporny na manipulacje.

– *Bezpieczeństwo nie może być kompromisem* – mówił **Wojciech Śnieżek z firmy Roger/Assa Abloy.**

Kierunek zmian wydaje się dziś wyraźny – od pojedynczych urządzeń do zintegrowanych platform bezpieczeństwa, które pozwalają szybciej reagować i budować spójny obraz sytuacji.

Pod napięciem – dosłownie

Film **„Pod napięciem”** otwierający konferencję zadawał ważne pytanie: co stanie się, jeśli system, który wydaje się niewidoczny i oczywisty, przestanie działać?

Po kilku godzinach rozmów odpowiedź wydawała się bardziej złożona niż na początku.

Bo bezpieczeństwo energetyczne nie zaczyna się w momencie awarii. Zaczyna się dużo wcześniej – od ludzi, decyzji, procedur, relacji i świadomości zagrożeń.

I być może właśnie to było najważniejszym wnioskiem całego wydarzenia: dziś odporność sektora energetycznego nie zależy już wyłącznie od technologii. Zależy od tego, czy potrafimy dostrzec zagrożenia, zanim staną się widoczne dla wszystkich.

Relacyjny charakter wydarzenia można było dostrzec także poza sceną – przestrzeń wystawiennicza przez cały dzień pozostawała miejscem rozmów, wymiany doświadczeń i dyskusji.

Dzięki współorganizatorowi wydarzenia – Taurus Ochrona – oraz partnerom technologicznym: CIAS, Hanwha Vision, Megavision, i Roger/ASSA ABLOY po raz kolejny udało się stworzyć przestrzeń do rzeczowej wymiany doświadczeń i merytorycznych rozmów. Bo właśnie tam, gdzie spotykają się doświadczenie, praktyka i różne perspektywy, najczęściej pojawiają się odpowiedzi na najważniejsze pytania o bezpieczeństwo.

Qr kod do filmu „Pod napięciem”

Jubileuszowa 10. edycja Security BootCamp

14 maja dawna fabryka samolotów w Mielnie na chwilę zmieniła kolor na... niebieski. Wszystko za sprawą uczestników jubileuszowej, **10. edycji Security BootCampu,** którzy pojawili się w charakterystycznych niebieskich bluzach.

Na miejscu nie zabrakło rywalizacji i praktycznych wyzwań przygotowanych przez partnerów wydarzenia: **Axis Communications, Genetec, CCTV Baltic, HID, Roger, Securitas oraz Ironsky.**

– *Wiosenna edycja Security BootCamp to szkolenie terenowe dla security managerów, podczas którego partnerzy technologiczni przygotowali zawody techniczne i konkurencje terenowe. Uczestnicy rywalizowali ze sobą, jednocześnie poznając najnowsze technologie w dziedzinie zabezpieczeń* – powiedział Mariusz Kucharski z a&s Polska.

Security BootCamp to jednak nie tylko zadania i technologia. To przede wszystkim przestrzeń do merytorycznych rozmów, wymiany doświadczeń oraz networkingu w wyjątkowej scenerii pełnej historii lotnictwa.

KONRAD BADOWSKI,
AXIS COMMUNICATIONS

– Nie zdawałem sobie sprawy, że to już dziesiąta edycja, więc ogromne gratulacje, ponieważ ta formuła jest naprawdę świetna. Pokazaliśmy pełną integrację technik radarowych, termowizyjnych, termometrycznych i wizyjnych. Dodatkowo w urządzeniach wizyjnych jesteśmy w stanie wykorzystywać także obraz z podczerwieni w ciągu dnia. Dzięki temu uzyskujemy niespotykany wcześniej kontrast na dużych odległościach.

MAREK SKOWRONEK,
SECURITAS POLSKA

– Pokazujemy narzędzie, które ma zachęcić grupę do dyskusji. W praktyce oznacza to przetłumaczenie międzynarodowej normy ISO 31000 na język codziennych decyzji. Inspirujemy uczestników do podejmowania decyzji razem z nami, zamiast czekania na to, co się wydarzy.

PIOTR ROGALEWICZ,
GENETEC

– Były to interaktywne ćwiczenia z zakresu wykrywania zagrożeń hybrydowych, szczególnie pod presją aktywnego strzelca. Wykorzystaliśmy laserowe trenażery replik broni. Za pomocą analityki pokazaliśmy, jak w praktyce przeprowadzić procedurę reagowania na tego typu zagrożenie. Było to połączenie wideomonitoringu, analizy wideo i kontroli dostępu.

JAROSŁAW OGRABEK,
BIOAGRA

– Partnerzy oraz osoby, które tutaj przyjechały, uczą się od siebie nawzajem bardzo wiele. To nowe rozwiązania, które z pewnością będą mogli spróbować wdrożyć w swoich firmach.

BARTOSZ WRÓBLEWSKI,
CCTV BALTIC

– Dla uczestników przygotowaliśmy escape room. Opracowaliśmy sekwencje do wprowadzenia w czytnikach, aby można było otworzyć ostatnie drzwi i wyjść. Uczestnicy musieli odnaleźć wszystkie wskazówki, wprowadzić odpowiednie kody, wydostać się z pomieszczenia, a następnie dotrzeć do naszego vana. Pokazaliśmy również, jak możemy pomóc w zabezpieczeniu obiektów oraz wesprzeć w rozwiązywaniu problemów pojawiających się w różnego rodzaju obiektach.

ŁUKASZ WDOWIAK,
ROGER ASSA ABLOY

– Przede wszystkim chcieliśmy poznać opinie prawdziwych ekspertów w tej dziedzinie. Jakie decyzje podjęliby w przypadku różnych incydentów, które mogłyby negatywnie wpłynąć na poziom bezpieczeństwa. Przygotowaliśmy scenariusz, w którym uczestnicy wcielili się w rolę managera security w nowoczesnym biurowcu, a ich zadaniem było zminimalizowanie potencjalnych strat. Myślę, że gra spodobała się uczestnikom, ponieważ są to ludzie, dla których bezpieczeństwo nie jest kosztem, lecz inwestycją.

TOMASZ CEBULA,
GAZ-SYSTEM

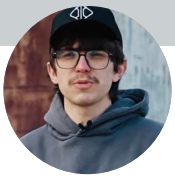
– Ze względu na to, że wszyscy zajmujemy się bezpieczeństwem, mierzymy się z podobnymi problemami. Dzięki rozmowom można usłyszeć inną perspektywę i poznać odmienne podejście do rozwiązywania problemów.

DARIUSZ DĘBSKI,
PORT GDYNIA

– Podobał mi się wysoki poziom wydarzenia oraz nowoczesne rozwiązania odpowiadające obecnym trendom w bezpieczeństwie, szczególnie w kontekście nowych dyrektyw. Może to przyczynić się do zwiększenia bezpieczeństwa, na przykład w portach morskich.

PAWEŁ LATEK,
HID GLOBAL

– Firma HID po raz pierwszy uczestniczyła w BootCampie. Bardzo interesującym punktem była rozmowa o Amico. Wielu uczestników pytało nas, jak dane są przechowywane, czy są zgodne z RODO oraz z polskim prawem. Oczywiście odpowiedź brzmi: tak. To jedynie ciąg znaków – bez znaków szczególnych, twarzy czy zdjęć. Dla zwykłego użytkownika są one całkowicie nierozpoznawalne.



WIKTOR KOŁODZIEJ,
IRONSKY

– Mieliśmy okazję zaprezentować flotę naszych dronów i ich możliwości. Skupiliśmy się na wykrywaniu ludzi, ale także różnych pojazdów i obiektów, pokazując również, jak można zautomatyzować ten proces. Przedstawiliśmy też robo-psa, który po odpowiednim zaprogramowaniu przez wyspecjalizowaną firmę jest w stanie bez problemu patrolować wnętrza budynków oraz hale.

ANNA AUGUSTYNIAK,
ID LOGISTICS

– Myślę, że takie wydarzenia są wspaniałym doświadczeniem i zawsze pozostawiają wiele inspiracji, ponieważ mamy okazję spotkać managerów z różnych branż. To otwiera umysł i pomaga w naszej codziennej pracy. I to jest fantastyczne.

Linc Polska

Camect już mówi...

HUB Camect wprowadza innowacyjne podejście do systemów monitoringu wizyjnego, podnosząc ich funkcjonalność na nowy poziom. Dzięki wykorzystaniu algorytmów sztucznej inteligencji do analizy obrazu w czasie rzeczywistym Camect potrafi wykrywać ludzi, pojazdy oraz ponad 30 innych typów obiektów. Nowością jest funkcja automatycznego generowania komunikatów audio na podstawie interpretacji zdarzeń rejestrowanych przez kamery.

Uwaga, mężczyzno w zielonej bluzie z kapturem, proszę oddalić się od samochodu i opuścić teren! Policja została powiadomiona!

Mechanizm ten umożliwia natychmiastowe ostrzeganie intruzów i aktywną reakcję systemu jeszcze przed próbą włamania lub wystąpieniem szkody. Integracja analizy wizyjnej z automatycznymi komunikatami głosowymi znacząco zwiększa skuteczność detekcji oraz prewencji zagrożeń.

Z psychologicznego punktu widzenia ogromne znaczenie ma fakt, że nieproszony gość zostaje zauważony, a jego cechy charakterystyczne są identyfikowane i komunikowane bezpośrednio do niego. Świadomość, że system obserwuje, analizuje i rejestruje działania w czasie rzeczywistym, działa silnie odstraszająco i bardzo często skutecznie zniechęca do kontynuowania niepożądanych działań.

Nowa funkcja audio znajduje zastosowanie m.in. w firmach, magazynach, na parkingach, budowach oraz posesjach prywatnych. Camect przekształca tradycyjny, pasywny monitoring w aktywny system bezpieczeństwa oparty na AI – taki, który nie tylko rejestruje zdarzenia, ale także automatycznie reaguje na zagrożenia i skuteczniej odstrasza potencjalnych intruzów. •

ROGER

RKD32-SE: większy komfort obsługi i wyższy poziom zabezpieczeń

Odświeżony depozytor kluczy RKD32-SE to prosty sposób na skuteczne zarządzanie obiegiem kluczy w organizacji – wiadomo, kto pobrał klucz, kiedy, na jak długo oraz czy został on zwrócony na czas.

Urządzenie automatycznie rejestruje wszystkie zdarzenia (pobrania, zwroty oraz dane użytkownika), dzięki czemu zapewnia pełną kontrolę i ułatwia audyty, bez ręcznie prowadzonych zeszytów i domysłów.

System pozwala precyzyjnie definiować uprawnienia, określając dostęp do konkretnych kluczy oraz przedziały czasowe ich pobrania. Obsługuje także podział na grupy „wewnętrzną" i „zewnętrzną", np. poprzez wymuszenie zwrotu kluczy zewnętrznych przed pobraniem klucza wewnętrznego. Dostępne są również funkcje rezerwacji oraz limitów wypożyczeń, co realnie zmniejsza przestoje i eliminuje „wąskie gardła" w utrzymaniu ruchu czy administracji obiektu.

Dla większej elastyczności dostępny jest także tryb biurowy, umożliwiający pobieranie i zwrot kluczy bez identyfikacji użytkownika.

W sytuacjach awaryjnych klucze mogą zostać odblokowane z poziomu panelu awaryjnego zabezpieczonego kluczem mechanicznym. Próby siłowego otwarcia drzwi lub obudowy są rejestrowane i mogą być sygnalizowane na zewnątrz, np. do systemu alarmowego.

W odświeżonej wersji urządzenie wyposażono w większy, 10-calowy panel sterujący oraz czytnik zbliżeniowy obsługujący szyfrowane sektory kart MIFARE®, co zwiększa wygodę obsługi i wzmacnia kontrolę identyfikacji.

Depozytor może działać samodzielnie lub w trybie sieciowym, a jeden panel może obsłużyć do czterech depozytorów, co ułatwia skalowanie systemu w większych lokalizacjach. •


check. create. manage.
Checly
Zakład produkcyjny
wszystkie lokalizacje
Zadania do wykonania
dla mnie
wszystkie
2 gru
Kontrola ochrony fizycznej
Krzysztof Pacel
3 gru
Inspekcja obiektu Południe
Zbigniew Koczwara
4 gru
Kontrola bramy głównej
Łukasz Bleniek
5 gru
Sprawdzenie czujek na wejściu
Jarosław Reguła
6 gru
Kontrola pracownika w recepcji
Franciszek Gola
Checly
the best startup 2023
checly.app

PulsON ALARM

NIKT NIE WEJDZIE NIEZAUWAŻONY

pulsonalarm.pl

PRODUKT POLSKI
POLSKA PRODUKCJA,
CHMURA I TECHNOLOGIA

Pierwsza innowacyjna centrala na rynku z wbudowanymi modułami komunikacyjnymi 4G LTE/2G, Wi-Fi i LAN