

**RAPORT: NOWA ERA
BEZPIECZEŃSTWA PUBLICZNEGO**

Tradycyjne podejście do ochrony przestaje być wystarczające. W erze realnych i cyfrowych incydentów Polska buduje inteligentną tarczę ochronną.

**SZTUCZNA INTELIGENCJA
W WIELKIM MIEŚCIE**

Wiele miast na całym świecie wykorzystuje sztuczną inteligencję, by zapewnić mieszkańcom bezpieczeństwo. Ale czy ceną za nie musi być nasza prywatność?

MOBILNE WIEŻE MONITORINGU

Wyzwania związane z ochroną osób czy przestrzeni wymagają rozwiązań gotowych do szybkiego wdrożenia. Na te potrzeby odpowiadają mobilne wieże monitorujące.



20 zł
(w tym 8% VAT)



7 LISTOPADA 2025

WARSAW **SECURITY** **SUMMIT**

NOWY TERMIN
NOWA FORMUŁA



WarsawSecuritySummit.online

Nowa era bezpieczeństwa publicznego

W roku 1961 opublikowana została książka *The Death and Life of Great American Cities* (*Śmierć i życie wielkich miast Ameryki*, wyd. pol. 2014). Jej autorką jest Jane Jacobs, dziennikarka magazynu „Architectural Forum”, nowojorczanka mocno zmartwiona tym, w którą stronę zmierza jej ukochane miasto. W Nowym Jorku walczyła z projektami wyburzeń dzielnic (m.in. Greenwich Village), blokując budowę autostrad przez dzielnice mieszkaniowe. Według Jacobs bezpieczeństwo ulicy zależy przede wszystkim od liczby oczu, które ją obserwują. Najlepszym sposobem zapewnienia tych oczu są sklepy, bary i inne miejsca publiczne, które przyciągają ludzi przez cały dzień. Od lat 70. sporo się jednak zmieniło. Czujne sąsiedzkie oko zostało zastąpione przez oko nie mniej czujnej kamery. Nie zmieniło się natomiast jedno – w każdej przestrzeni publicznej, czy będzie to ulica, czy też plac lub duże centrum handlowe, chcemy się czuć chronieni. Teraz jednak nie oczekujemy, że ochrona polegać będzie wyłącznie na fizycznej obecności służb mundurowych. Konwencjonalne metody nadzoru ustępują zatem miejsca systemowi techniczno-organizacyjnemu. W obecnym wydaniu „a&s Polska” przedstawiamy panoramę tej transformacji, której skutki odczuwamy już dziś. Więcej w artykule *Nowa era bezpieczeństwa publicznego*, na str. 12.

Ta transformacja nie eliminuje tradycyjnych form działania służb, lecz prowadzi do głębokiej integracji z technologiami GIS, *big data* oraz mobilnymi aplikacjami koordynującymi działania ratunkowe. Cyfryzacja ochrony zaciera granicę między domeną fizyczną a wirtualną. Ewolucja ku specjalistycznym wieżom obserwacyjnym wyposażonym w czujniki akustyczne i systemy wideoanalizy, wspieranym przez mobilne drony z kamerami termowizyjnymi, wyznacza kierunek przemian w całym sektorze bezpieczeństwa, czego dowodem choćby systemy zabezpieczeń stosowane na granicach naszego kraju (*Bezpieczna granica*, str. 18).

Fundamentalne pozostaje jednak zagadnienie, że nawet najbardziej wyrafinowane technologie nie zastąpią przemyślanego projektowania przestrzeni publicznej (*Bezpieczne miasto jest dobrze pomyślane*, str. 26). Właściwe oświetlenie, czytelny układ komunikacyjny i strategicznie rozmieszczone punkty styku dla patroli policyjnych tworzą w harmonii z systemami wideo-analitycznymi skuteczną tarczę ochronną.

Skonsolidowane platformy łączące dane z monitoringu wizyjnego, czujników jakości powietrza i inteligentnego oświetlenia ilustrują przyszłość zarządzania bezpieczeństwem miejskim. Jednolite centra dowodzenia umożliwiają służbom równoczesną obserwację ruchu pojazdów, prognozowanie natężenia ruchu pieszego i automatyczne reagowanie na anomalie. O tym wszystkim przeczytać można w artykule *Sztuczna inteligencja w wielkim mieście*, str. 34.

Współczesne bezpieczeństwo publiczne wykracza daleko poza tradycyjne rozumienie ochrony przed przestępczością. Zabezpieczenie łańcucha dostaw żywności, o czym piszemy na str. 64 w artykule *Sabotaż na talerzu*, wymaga precyzyjnych analiz chemicznych, systemów szacowania ryzyka i ścisłych procedur kontrolnych, minimalizujących potencjalne kryzysy biologiczne i chemiczne.

Przyszłość bezpieczeństwa publicznego zależy od synergii między tradycyjnymi kompetencjami służb a nowoczesnymi rozwiązaniami technologicznymi. To proces tworzenia nowych form współpracy, w których ludzkie doświadczenie i intuicja wspierane są przez możliwości analityczne sztucznej inteligencji. Transformacja ta wymaga jednak przemyślenia procedur, budowania świadomości społecznej oraz znajdowania równowagi między bezpieczeństwem a prawami podstawowymi obywateli. •

Redakcja

ZŁOTY PARTNER A&S POLSKA

BCS

Linc
Polska Sp. z o.o.

smart-i

SREBRNY PARTNER A&S POLSKA

HIKVISION

A&S POLSKA WYDANIE ONLINE: aspolska.pl



Spis treści

8 Produkty numeru

BEZPIECZEŃSTWO PUBLICZNE

- 12 **Nowa era bezpieczeństwa publicznego.
Technologia w służbie państwa**
Adela Prochyra
- 18 **Bezpieczna granica – od prostych rozwiązań
po zaawansowane systemy**
Monika Żuber-Mamakis
- 26 **Bezpieczne miasto jest dobrze pomyślane**
Monika Żuber-Mamakis
- 32 **Nowoczesne technologie zapewniają bezpieczeństwo
na ulicach i w obiektach**
Herz
- 33 **Jak przeciwdziałać zagrożeniom w przestrzeni publicznej**
Wywiad z Arturem Hejdyszem, C&C Partners
- 34 **Sztuczna inteligencja w wielkim mieście**
Jan T. Grusznic
- 38 **Civileo Smart City – przyszłość zarządzania
bezpieczeństwem w miastach i gminach**
Oke
- 40 **Smart city bezpieczne dzięki narzędziom Hikvision**
Michał Swoboda, Hikvision Poland
- 42 **Bezprecedensowe środki bezpieczeństwa w Watykanie**
Monika Żuber-Mamakis

REDAKCJA

ADRES REDAKCJI
a&s Polska
ul. Żłoczowska 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

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

© Copyright by a&s Polska

BCS
MOBILCAM

NIEZAWODNA MOBILNA OCHRONA

CHROŃ LUDZI, MIEJSCA
I ZASOBY Z WIEŻĄ **BCS**
MOBILCAM

MOBILCAM ZWIĘKSZY
BEZPIECZEŃSTWO
OBSZARU LUB OBIEKTU



www.bcs.pl
www.facebook.com/bcscctvpl



Spis treści

44 Czy bezbiletowe parkingi Freeflow to przyszłość parkowania w miastach?

Designa

46 Za kulisami bezpiecznej imprezy

Paweł Korzybski, PZPO

47 Kamery nasobne w ofercie ASBIS: innowacyjne rozwiązanie dla służb i ratowników

Wywiad z Tomaszem Mąkowskim, Asbis

48 Czy stanie na stacji lokomotywa?

Monika Żuber-Mamakis

54 Sabotaż na talerzu? Żywność jako broń XXI wieku

Jacek Tyburek

58 Głos branży

RYNEK SECURITY

63 Mobilne wieże monitoringu

Krzysztof Bereza, PZPO

64 LivEye – SMART BY DAY, SECURE BY NIGHT

Liveye

65 Mobilne wieże monitoringu firm: BCS, Janex, Securitas, Uniforce, VCS

68 Mapa inwestycji

Adela Prochyra

SERWIS INFORMACYJNY

70 Ster na bezpieczeństwo – Bootcamp z widokiem na morze

74 Public Safety Conference 2025: granice, technologie, procedury. Jak wygląda bezpieczeństwo publiczne w Polsce?

76 Informacje firmowe/nowości produktowe



Dla firm



tu jest



Centrum Doświadczeń Cyberbezpieczeństwa

**Ucz się z nami, jak lepiej chronić
swoją firmę przed cyberatakami**



Budowanie bezpieczniejszego społeczeństwa cyfrowego nie jest możliwe w pojedynkę, wymaga wysiłku zespołowego. Osoby decyzyjne nie mogą zwiększyć bezpieczeństwa cyfrowego organizacji bez zaangażowania całej firmy.

Nasze Centrum Doświadczeń Cyberbezpieczeństwa mieści się w Miasteczku Orange w centrum Warszawy. Stworzyliśmy je dla klientów, aby mogli lepiej zrozumieć wyzwania dzisiejszej cyberprzestrzeni. Wykorzystujemy przy tym wizualizację i wprowadzamy reguły jak w grze decyzyjnej, aby w ciekawy sposób zaprezentować korzyści płynące z długoterminowej strategii w zakresie cyberbezpieczeństwa.

Koncentrujemy się na osobach decyzyjnych w firmie i pomagamy im lepiej zrozumieć różne problemy, ale też potrzeby związane z budowaniem cyberodporności.

Kontakt: Daniel Kamiński daniel2.kaminski@orange.com



Prezentujemy najnowsze urządzenia z oferty firm

BCS, HIKVISION, IFTER, LINC, TP-LINK



BCS

Rejestratory BCS Point z technologią AcuSearch

Nowa technologia zautomatyzowanego wyszukiwania nagrań AcuSearch to rewolucyjne rozwiązanie, z którym odnalezienie poszukiwanego obiektu lub osoby staje się wyjątkowo proste i szybkie. Wystarczy zaznaczyć interesującą nas sylwetkę na obrazie – podczas podglądu na żywo lub odtwarzania nagrań – kliknąć „Szukaj” i gotowe. Konkretnie fragmenty nagrań zawierające najbardziej podobne do niego obiekty pojawiają się w ciągu kilku sekund.

To, co kiedyś zajmowało godziny żmudnego przeglądania materiałów wideo, teraz odbywa się błyskawicznie, znacznie przyspieszając prowadzenie dochodzeń i interwencji.

Rejestratory BCS Point z technologią AcuSearch potrafią z ogromną precyzją wyodrębnić atrybuty wykrytych obiektów nawet w trudnych warunkach. Dzięki temu możliwe jest późniejsze wyszukiwanie osób, podając jedynie ich opis. Analiza materiałów ze wszystkich kanałów jednocześnie i porównanie danych, znacząco zmniejsza ryzyko popełnienia przez system błędu oraz diametralnie skraca czas identyfikacji poszukiwanego obiektu. Umożliwia to szybszą reakcję służb na zdarzenie, co przekłada się na bezpieczeństwo mieszkańców czy pracowników.

Rejestratory BCS Point z funkcją zautomatyzowanego wyszukiwania AcuSearch są już dostępne na rynku w przystępnej cenie, co czyni je doskonałym wyborem dla firm poszukujących nowoczesnych, a zarazem ekonomicznych rozwiązań. •

Więcej na: www.bcs.pl



HIKVISION

Guanlan – wielkoskalowe modele AI

Firmy coraz częściej sięgają po technologie AIoT, aby sprostać wyzwaniom operacyjnym i przyspieszyć transformację cyfrową. Wychodząc naprzeciw tym potrzebom, Hikvision wprowadza wielkoskalowe modele AI Guanlan.

Wielkoskalowe modele AI Guanlan opierają się na trójwarstwowej architekturze, obejmującej modele bazowe, takie jak duże modele wizyjne, językowe i multimodalne, modele branżowe na warstwie pośredniej oraz modele zadaniowe na najwyższym poziomie. Taką strukturę zaprojektowano z myślą o spełnianiu szerokiego zakresu potrzeb – od podstawowych funkcji po złożone zastosowania scenariuszowe. Dzięki temu możliwe jest tekstowe poinstruowanie rejestratora czego ma szukać, np. „mężczyzna w koszuli w kratę”, „kobieta z wózkiem dziecięcym”, „osoba na spacerze z psem”, itp. Dzięki wielkoskalowemu modelowi sztucznych sieci neuronowych rejestrator wyszukuje w zapisanym materiale fragmentów obrazu, które pasują do zadanych kryteriów zarówno pod względem obiektów, jak i czynności, które wykonują.

Kamery DeepinViewX, wykorzystując potęgę wielkoskalowych modeli Guanlan, znacząco podnoszą standardy analizy treści materiału wizyjnego (VCA). Dzięki temu zasięg detekcji jest dwukrotnie większy, liczba powtarzających się alarmów spada o połowę, a skuteczność wykrywania wzrasta. Co więcej, liczba fałszywych alarmów na obwodzie została zredukowana o ponad 90% w porównaniu do tradycyjnych rozwiązań AI.

Pełne portfolio AIoT obejmie kamery termowizyjne HeatPro-Series oraz kamery Intelligent Checkpoint – oba modele wzbogacone o niezrównaną dokładność modelu Guanlan. •

Więcej na: www.hikvision.com/pl/

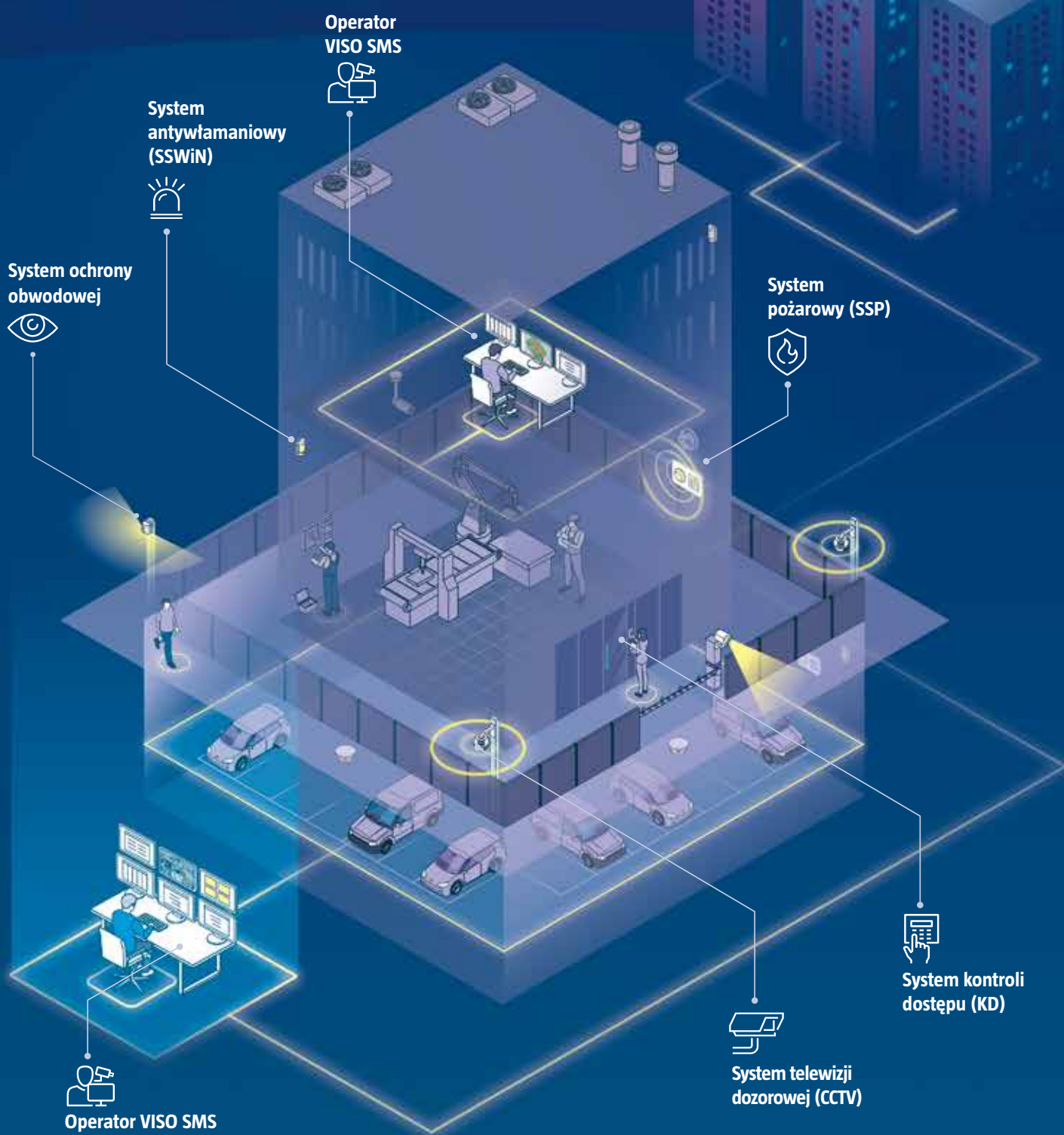
VISO SMS

Monitorowanie i wizualizacja systemów bezpieczeństwa

roger

Intelligence for Building

- Integracja z systemami Bosch, Dahua, Hikvision, Honeywell, Milestone, SATEL, Siemens i innymi w ramach jednej platformy
- Monitorowanie, wizualizacja i lokalizacja alarmów oraz innych zdarzeń na mapach
- Jednoczesna obsługa systemu przez wielu operatorów
- Efektywne zarządzanie personelem ochrony na obiekcie
- Przejrzysty interfejs użytkownika





IFTER

IFTER EQU2 – integracja z systemami BMS

System do integracji i wizualizacji systemów zabezpieczeń oraz automatyki budynkowej IFTER EQU2 został rozszerzony o obsługę dwóch nowych protokołów komunikacyjnych: IEC104 oraz DNP3. Są to standardy komunikacyjne powszechnie wykorzystywane w sieciach dystrybucyjnych energetyki do przesyłania danych pomiędzy systemami nadzoru. Ich implementacja umożliwia firmom energetycznym zarządzanie urządzeniami w sieci energetycznej bezpośrednio z poziomu systemu SCADA, a także – co kluczowe – zarządzanie systemami zabezpieczeń w ramach tychże systemów.

IFTER EQU2 obsługuje już ponad 100 różnych integracji w zakresie systemów zabezpieczeń, w tym: sygnalizację pożarową, kontrolę dostępu, sygnalizację włamania i napadu oraz telewizję dozorową. Komunikując się z tymi systemami IFTER EQU2 odczytuje ich bieżące stany oraz zdarzenia, w tym alarmowe. Następnie konwertuje te informacje na protokoły IEC104 lub DNP3, czyniąc je zrozumiałymi dla systemów SCADA. To właśnie pozwala na wizualizację systemów zabezpieczeń – obok urządzeń energetycznych – na planach stacji elektroenergetycznych w systemie SCADA.

Co więcej, z poziomu SCADA jest również możliwe pobieranie struktury urządzeń z IFTER EQU2, kompleksowa obsługa alarmów z systemu zabezpieczeń oraz zdalne sterowanie, np. blokowanie drzwi czy uzbrajanie/rozbrajanie stref alarmowych. Dzięki tak roz-

budowanym możliwościom integracyjnym systemu IFTER EQU2 możliwe jest znaczce podniesienie poziomu bezpieczeństwa w energetycznych sieciach dystrybucyjnych. •

Więcej na: www.ifter.com.pl



LINC POLSKA

Nowe bispektralne kamery termowizyjne serii 35 i 60 marki Honeywell



Bispektralne kamery termowizyjne Honeywell rejestrują jednocześnie zarówno sygnały termowizyjne, jak i wizyjne, dając szczegółowe obrazy osób lub obiektów znajdujących się w większej odległości w warunkach słabego oświetlenia. Pozwala to na szybszą reakcję na potencjalne zagrożenia.

Kamery te są idealne do zastosowań w infrastrukturze krytycznej, usługach, obiektach handlowych, magazynach i centrach logistycznych, stacjach ładowania pojazdów elektrycznych oraz elektrowniach słonecznych.

Modele obu serii mają rozdzielczość optyczną 5 Mpix, szeroki zakres ogniskowych, wytrzymałą konstrukcję IK10. Zaawansowana analityka umożliwia wykrywanie istot żywych, przegrzewającego się sprzętu, dymu, punktów zapalnych pożaru i otwartego ognia. Inne funkcje analityczne obejmują m.in. detekcję pojazdów z analizą przekroczenia pojedynczych i podwójnych linii oraz wykrywanie jazdy pod prąd, np. w zastosowaniach perymetrycznych i kontroli granicznej.

Serie różnią się przede wszystkim przetwornikiem termowizyjnym, którego rozdzielczość wynosi 256 x 192 dla serii 35 oraz 640 x 512 dla serii 60. Dodatkowo seria 60 ma unikatową konfigurowalną funkcję ostrzeżeń głosowych do wczesnego ostrzegania o konieczności opuszczenia obszaru.

Seria 35 obejmuje bispektralne kamery typu „bullet” HC35TB5R1JT07 i HC35TB5R4JT10 oraz kamery cylindryczne HC35TE5R3JT21 i HC35TE5R4JT35, natomiast seria 60 pięć modeli kamer typu „bullet” HC60TB4R1VT09, HC60TB4R4VT15, HC60TB4R2VT25, HC60TB4R2VT35 i HC60TB4R2VT50. •

Więcej na: www.linc.pl



TP-LINK

EAP725-Wall – Punkt dostępowy Wi-Fi 7 w kompaktowej obudowie

TP-Link EAP725-Wall to urządzenie, które łączy wydajność standardu Wi-Fi 7 z eleganckim designem. Idealnie sprawdzi się w zastosowaniach biznesowych i domowych.

Urządzenie oferuje wyjątkową wydajność dzięki dwuzakresowej technologii, osiągając prędkości do 688 Mb/s w paśmie 2,4 GHz oraz imponujące 2882 Mb/s w paśmie 5 GHz, co gwarantuje stabilne i szybkie połączenie niezależnie od obciążenia sieci. Dużym atutem urządzenia jest pełna kompatybilność

z platformą Omada SDN do centralnego zarządzania całą infrastrukturą sieciową przez chmurę.

Punkt dostępowy został wyposażony w rozbudowaną sekcję portów, obejmującą port uplink Ethernet 2,5G oraz trzy porty dla urządzeń końcowych: jeden port Ethernet 2,5G i dwa porty gigabitowe. Zastosowanie zaawansowanych rozwiązań technologicznych, takich jak kanał o szerokości 160 MHz, 1024-QAM, długi symbol OFDM czy technologie MU-MIMO i OFDMA, gwarantuje stabilne i płynne działanie



nawet w warunkach dużego obciążenia sieci. Funkcja płynnego roamingu Wi-Fi oraz Omada Mesh umożliwiają bezproblemowe przemieszczanie się między punktami dostępowymi oraz bezprzewodowe łączenie urządzeń, tworząc spójną i wydajną sieć.

Urządzenie zostało zaprojektowane z uwzględnieniem potrzeb nowoczesnych przestrzeni biznesowych, takich jak biura czy hotele, gdzie dyskretny wygląd i wydajność są równie ważne – EAP725-Wall posiada niezwykle kompaktową obudowę o wymiarach: 86 mm szer., 143 mm wys., i 40 mm gr.

TP-Link EAP725-Wall jest już dostępny w sprzedaży, został objęty 5-letnią gwarancją producenta. •

Więcej na: www.tp-link.com/pl/

[ADRESOWALNY
KOMPAKTOWY]

POLON 3000



SYSTEM SYGNALIZACJI POŻAROWEJ



NIEZAWODNOŚĆ

System szybko wykrywa zagrożenie pożarowe, minimalizując ryzyko strat.



ŁATWOŚĆ INSTALACJI

Kompaktowa budowa pozwala na szybki i nieskomplikowany montaż, a także oszczędność miejsca.



SKALOWALNOŚĆ

Możliwość dostosowania do specyficznych potrzeb obiektu, co gwarantuje maksymalną ochronę.



OPŁACALNOŚĆ

POLON 3000 to przystępna inwestycja w bezpieczeństwo, która zwraca się w postaci bezcennego spokoju.

Zadbaj o bezpieczeństwo swojego obiektu już dziś!



Nowa era bezpieczeństwa publicznego

Technologia w służbie państwa

W czasach, gdy granice przekraczają nie tylko ludzie, ale i dane, a bezpieczeństwo infrastruktury transportowej mierzy się zarówno w kilometrach, jak i w terabajtach, Polska stawia na technologię. Od dróg monitorowanych z powietrza, przez kolej sterowaną cyfrowo, po granice naszpikowane sensorami – ten raport pokazuje, jak państwo buduje inteligentną tarczę ochronną w erze realnych i cyfrowych zagrożeń.

Adela Prochyra





B

Bezpieczeństwo publiczne jeszcze nigdy nie było tak bardzo powiązane z rozwojem technologii, jak w pierwszych dekadach XXI wieku. W czasach, gdy zagrożenia mogą nadejść z przestrzeni realnej i wirtualnej, a infrastruktura państwa staje się celem zarówno fizycznych ataków, jak i cyberprzestępczości, tradycyjne podejścia do ochrony przestają być wystarczające. Państwa muszą budować nowe, wielowymiarowe systemy zabezpieczeń – szybkie, zautomatyzowane i zdolne do działania w czasie rzeczywistym.

Obecnie bezpieczeństwo infrastruktury transportowej i granicznej przestaje być wyłącznie domeną fizycznej obecności służb i prostych narzędzi kontrolnych. Coraz częściej opiera się na integracji zaawansowanych technologii, zdalnych systemów nadzoru oraz automatyzacji procesów reagowania i wykrywania zagrożeń. Raport ten przedstawia aktualny stan oraz kierunki rozwoju zabezpieczeń w trzech strategicznych obszarach państwa – drogach publicznych, sieci kolejowej i granicach – analizując zarówno rozwiązania systemowe, jak i rolę nowoczesnych narzędzi, takich jak drony czy inteligentne platformy analityczne.

Drogi pod cyfrowym nadzorem

Współczesne podejście do bezpieczeństwa drogowego w Polsce jest już dalekie od jakże analogowego systemu składającego się wyłącznie ze znaków drogowych i sygnalizacji świetlnej oraz przepisów ruchu drogowego. Od kilkunastu lat opiera się ono na synergii różnych zaawansowanych technologii i narzędzi. Integracja systemów ITS (Inteligentny System Transportowy) i OPP (Odcinkowy Pomiar Prędkości) oraz wykorzystanie dronów pozwala na skuteczniejsze monitorowanie sytuacji na drogach, szybszą reakcję na incydenty oraz lepsze planowanie działań prewencyjnych.

W największych polskich miastach w powszechnym użyciu są ITS, czyli inteligentne systemy integrujące różne technologie i urządzenia. Na bieżąco zbierają i przetwarzają dane z czujników ruchu, kamer oraz systemów informacji pasażerskiej, umożliwiając dynamiczne zarządzanie sygnalizacją świetlną i informowanie kierowców o aktualnych warunkach na drogach. Mniejsze systemy można znaleźć także w dziesiątkach mniejszych polskich miast – m.in. elektroniczne tablice parkingowe informujące o dostępnych miejscach, systemy dynamicznej informacji pasażerskiej.

Na drogach międzymiastowych stosowane są różnego rodzaju zabezpieczenia fizyczne, jak bariery energochłonne, oznakowanie poziome i pionowe o wysokiej odbliaskowości, a także fotoradary

czy odcinkowe pomiary prędkości (OPP). Zwłaszcza te ostatnie to bardzo skuteczne narzędzie w walce z nadmierną prędkością na drogach. Systemy te, poprzez rejestrację czasu przejazdu między dwoma punktami, obliczają średnią prędkość pojazdu na danym odcinku. Zbierają dane z dokładnością do 10 km/h, a za przekroczenie limitu prędkości automatycznie wystawiają mandat. Obecnie w Polsce zainstalowanych jest ok. 70 OPP, ale Centrum Automatycznego Nadzoru nad Ruchem Drogowym planuje instalację kolejnych, w tym na autostradach A1 i A2. Dane z CANARD pokazują, że na odcinkach objętych OPP liczba wypadków spadła o 57%, liczba ofiar śmiertelnych o 71%, a liczba osób rannych zmniejszyła się o 56%.

Oczywiście, same systemy nie zapewnią bezpieczeństwa. Do egzekwowania przepisów potrzebni są ludzie. Tym zajmują się policja drogowa oraz Inspekcja Transportu Drogowego (ITD), które to służby intensyfikują działania kontrolne, wykorzystując nowoczesne technologie. Mobilne jednostki diagnostyczne ITD umożliwiają przeprowadzanie szczegółowych kontroli technicznych pojazdów bezpośrednio na drodze, co pozwala na szybkie wykrycie usterek i zapobieganie potencjalnym zagrożeniom. Dodatkowo, służby korzystają z przenośnych rejestratorów wideo oraz nieoznakowanych radiowozów wyposażonych w wideorejestratory, co pozwala na skuteczne dokumentowanie wykroczeń i zwiększa efektywność działań prewencyjnych. Problem jedynie w tym, że policja mierzy się z ogromną liczbą wakatów. 1 marca 2025 r. w całej Polsce brakowało niemal 14,5 tys. policjantów, czyli ok. 13% kadry (za: policja.pl, dostęp: 09.05.2025). Na tak dużą liczbę wakatów miało wpływ m.in. pojawienie się 500 nowych etatów dla Centralnego Biura Zwalczania Cyberprzestępczości.

Od ponad 10 lat policja wykorzystuje w swoich działaniach Bezzałogowe Statki Powietrzne (BSP), czyli drony, a w ruchu drogowym od 5 lat (za: „Kwartalnik Policyjny” 1/2024). Drony wykorzystywane przez policję drogową służą do monitorowania natężenia ruchu i identyfikacji przyczyn zatorów, co umożliwia m.in. organizowanie objazdów. Policyjne BSP wyposażone są w 30-krotny zoom optyczny i 180-krotny zoom cyfrowy. Funkcjonariusze używają ich również do rejestrowania wykroczeń kierowców, takich jak nieprawidłowe wyprzedzanie, nieustąpienie pierwszeństwa pieszym czy używanie telefonu podczas jazdy. Dodatkowo drony monitorują zachowanie rowerzystów i pieszych, w tym przestrzeganie sygnalizacji świetlnej oraz przechodzenie

”

W czasach, gdy zagrożenia mogą nadejść z przestrzeni realnej i wirtualnej, a infrastruktura państwa staje się celem zarówno fizycznych ataków, jak i cyberprzestępczości, tradycyjne podejścia do ochrony przestają być wystarczające.



w miejscach niedozwolonych. Praktycznych zastosowań BSP jest oczywiście o wiele więcej, jak chociażby nadzór nad bezpieczeństwem masowych wydarzeń sportowych czy przejazdów delegacji państwowych.

Kolej na bezpieczeństwo. Jak cyfrowa modernizacja chroni sieć kolejową

Od czego zależy bezpieczeństwo kolei? Między innymi od dobrych systemów zabezpieczających ruch pociągów. Powszechnie stosowane są na kolei systemy sterowania ruchem kolejowym – SRK, które odpowiadają za bezpieczne przemieszczanie się pociągów po trasach i obejmują: systemy sygnalizacji, systemy sterowania przejazdami, systemy kontroli prędkości i inne elementy związane z ruchem pociągów. Obecnie systemy bezpieczeństwa sieci kolejowej w Polsce są intensywnie modernizowane, głównie w ramach Krajowego Programu Kolejowego do 2030 r. (z perspektywą do roku 2032). Od początku jego realizacji (2015 r.) do końca 2023 r. zakończono 212 projektów o łącznej wartości 28 686 497,7 tys. zł.

Jednym z jego najważniejszych projektów infrastrukturalnych jest stopniowa implementacja Europejskiego Systemu Zarządzania Ruchem Kolejowym (ERTMS – *European Rail Traffic Management System*), w tym podsystemu ETCS poziomu 2. To zaawansowane rozwiązanie technologiczne umożliwia elektroniczne sterowanie ruchem pociągów, ich stałe pozycjonowanie oraz automatyczną kontrolę prędkości, co w znaczący sposób ogranicza ryzyko błędu ludzkiego i zwiększa przepustowość linii. System ETCS poziomu 2 jest obecnie instalowany m.in. na modernizowanych odcinkach linii E20 (Warszawa–Terespol) oraz E65 (Warszawa–Gdynia), które należą do europejskich korytarzy transportowych. Równolegle rozwijana jest koncepcja Lokalnych Centrów Sterowania (LCS), które centralizują nadzór nad ruchem na długich odcinkach linii kolejowych. W 2025 r. funkcjonuje już ponad 50 LCS, a ich dalsze uruchomienia zaplanowano w ramach projektów unijnych współfinansowanych przez Connecting Europe Facility (pol. Instrument „Łącząc Europę”) i Fundusz Spójności.

Nie mniej istotnym aspektem bezpieczeństwa kolei jest ochrona infrastruktury przed aktami wandalizmu i sabotażu. Szczególną uwagę zwraca się na przejazdy kolejowo-drogowe, które są miejscami newralgicznymi z punktu widzenia bezpieczeństwa publicznego. W ostatnich latach PKP PLK we współpracy z Ministerstwem Infrastruktury zainstalowały systemy monitoringu na setkach przejazdów kolejowych w miejscach o wysokim



ryzyku zdarzeń. Istotną rolę odgrywa także Straż Ochrony Kolei (SOK), która dysponuje flotą mobilnych jednostek terenowych, wyposażonych w nowoczesny sprzęt, w tym kamery nasobne, systemy GPS i tablety z dostępem do baz danych. Coraz częściej SOK współpracuje również z analitykami danych i wykorzystuje rozwiązania predykcyjne, co pozwala kierować patrole w miejsca o najwyższym potencjale zagrożenia.

Na kolei coraz śmielej wkraczają również nowe technologie z zakresu inspekcji i nadzoru. PKP PLK testuje i wdraża zdalne systemy kontroli infrastruktury – w tym drony, które pozwalają szybko i bezpiecznie ocenić stan postępów budowy w nowych inwestycjach, a także torowisk, mostów, wiaduktów, tuneli czy rozjazdów. W 2024 r. uruchomiono w Małopolsce program pilotażowy z udziałem bezzałogowych statków powietrznych wyposażonych w kamery termowizyjne i czujniki strukturalne, które analizują stan techniczny obiektów inżynierskich oraz wykrywają potencjalne anomalie. Takie rozwiązania pozwalają na bieżąco planować prace utrzymaniowe i minimalizować ryzyko awarii. Obecnie w zasobach PKP PLK znajduje się ponad 30 dronów do zadań inspekcyjnych, a liczba ta systematycznie rośnie.

Oczywiście, wszystkie te elementy mogą paść ofiarami cyberprzestępców. Wydarzenia z 17 marca 2022 r., kiedy to awaria systemu Radio-Stop wyłączyła z użytku 19 LCS, uwiaryściły potrzebę większej uwagi na te kwestie w sektorze kolejowym. Choć LCS zarządzają ruchem na wielu stacjach i są zdalnie sterowane, ich zabezpieczenia oraz różnorodność używanych systemów (np. Alstom/Bombardier, Thales) stanowią barierę dla potencjalnych hakerów. Bardziej realnym zagrożeniem niż skomplikowane cyberataki są manipulacje fizyczne, takie jak przekierowanie prądu w obwodach torowych czy ręczne przestawianie rozjazdów. Dlatego kolej coraz chętniej stawia na rozwiązania typu przejazdu bezkolizyjnego (tunele, wiadukty) czy systemy automatyczne, które nie są podłączone do sieci.

Granice przyszłości. Nowoczesna tarcza ochronna Polski

Współcześnie bezpieczeństwo granic Polski wiąże się z zupełnie nowymi wyzwaniem niż jeszcze 10 lat temu, a jednocześnie nadal sprowadza się do skutecznego nadzoru nad ruchem osób, pojazdów i towarów. Granica przestaje być tylko linią lądowo-morską, a staje się systemem dynamicznego monitorowania, reagowania i prognozowania, który coraz częściej przypomina organizm autonomiczny, zdolny do adaptacji i działania w czasie rzeczywistym.

Polska granica wschodnia stanowi w większości granicę zewnętrzną Unii Europejskiej, dlatego jej ochrona wymaga ścisłej współpracy międzynarodowej. Jako członek Frontex, Polska uczestniczy w operacjach wspólnej ochrony i wymianie danych z agencjami UE, takimi jak Europol. Zarządzanie granicami wspierane jest systemami informacyjnymi, m.in. SIS (baza danych osób i przedmiotów poszukiwanych), VIS (system wizowy), EURODAC (rozpoznawanie odcisków palców) i EUROSUR (monitorowanie granic). Dodatkowo UE wdraża nowe narzędzia, jak System Wjazdu/Wyjazdu (EES) i ETIAS, które mają zautomatyzować kontrole i zwiększyć skuteczność wykrywania zagrożeń.

Środowisko prawne (przepisy, strategie itd.) to jedno, ale skuteczność ochrony granic państwa zależy w dużej mierze od sprawnie działających (fizycznych) systemów wykrywania zagrożeń

i reagowania na nie. W związku z rosnącymi napięciami geopolitycznymi oraz nasilającymi się zjawiskami migracyjnymi na wschodniej flance Unii Europejskiej ochrona granic obejmuje nie tylko tradycyjne działania patrolowe, lecz również zaawansowane systemy detekcji, obserwacji i reagowania – w dużej mierze oparte na automatyzacji, analizie danych i rozpoznaniu z powietrza. Na granicy z Białorusią, wzdłuż ponad 186 km pasa przygranicznego, w 2023 r. ukończono budowę nowoczesnej bariery fizyczno-elektronicznej. Składa się ona z 5,5-metrowego ogrodzenia stalowego wyposażonego w systemy detekcji i perymetrii: czujniki drgań, sejsmometry oraz kamery dzienne i termowizyjne, podłączone do Centrum Nadzoru w Białymstoku. System ten pozwala na całodobową obserwację oraz natychmiastowe wykrywanie prób nielegalnego przekroczenia granicy. W przypadku incydentu sygnał automatycznie trafia do operatorów monitoringu i patrolu terenowego, co znacząco skraca czas reakcji.

Oprócz tego zmodernizowany w latach 2022-24 system zabezpieczeń obejmuje system dróg dojazdowych, wież obserwacyjnych i flotę statków bezzałogowych. Na odcinku granicy z Białorusią rotacyjnie służy 8 tys. żołnierzy, policjantów i funkcjonariuszy Straży Granicznej. Ich pracę od lat wspierają technologie bezzałogowe – obecnie w Straży Granicznej wykorzystuje się łącznie ok. 50 płatowców i wirnikowców, a flota ta miała się powiększyć o 32 zestawy wirnikowców w 2024 r. i dwa zestawy płatowców w 2025 r. Potencjał sprzętowy Straży Granicznej ma zostać zwiększony o nowe pojazdy obserwacyjne PJN z kamerami dziennymi, termowizyjnymi i głowicami optoelektronicznymi, umożliwiającymi rozpoznanie osób z dużej odległości, także w nocy, bez wychodzenia z pojazdu. Planowany jest również zakup dwóch



Polska mimo wielu opóźnień i niedostatków konsekwentnie buduje wielowarstwowy, zintegrowany system bezpieczeństwa obejmujący kluczowe obszary transportu i ochrony granic.

samolotów Turbolet i czterech śmigłowców – obecnie flota SG liczy 10 samolotów i 8 śmigłowców.

Szczególne nadzoru wymaga także granica wodna. Morski Oddział Straży Granicznej dysponuje ponad 50 jednostkami pływającymi różnego typu, a w ramach programu modernizacji planowany jest zakup dwóch poduszkowców, które miały trafić do służby w 2024 r. Granicy morskiej strzeże także Zautomatyzowany System Radarowego Nadzoru (ZSRN), obejmujący całe polskie wybrzeże – od Świnoujścia po Piaski. To trójpoziomowa infrastruktura, składająca się z Posterunków Obserwacyjnych wyposażonych w radary Terma Scanter 200ITD, kamery termowizyjne, dalmierze laserowe oraz systemy łączności. Dane z posterunków trafiają do Lokalnych i Dywizyjnych Ośrodków Nadzoru, a następnie do Centralnego Ośrodka Nadzoru w Gdańsku, gdzie są integrowane z informacjami m.in. z Marynarki Wojennej i Urzędu Morskiego. Dzięki temu ZSRN zapewnia kompleksowy, aktualizowany w czasie rzeczywistym obraz sytuacji nawodnej, wspierając ochronę granic, środowiska oraz operacje poszukiwawczo-ratownicze. System działa od 2014 r., jednak ze względu na intensywne użytkowanie i rozwój technologii wymaga obecnie modernizacji i rozbudowy.

Drony na służbie państwa

Bezzałogowe statki powietrzne (BSP) są dziś wszechstronnym narzędziem wykorzystywanym przez różne służby państwowe – od policji, przez Straż Graniczną, po kolej i wojsko. Służą do wykrywania przestępstw, monitorowania ruchu drogowego, inspekcji infrastruktury technicznej oraz patrolowania granic, zwłaszcza w trudno dostępnych terenach. Policja używa dronów

do rejestrowania wykroczeń i wspierania akcji ratunkowych, kolej – do inspekcji torów i linii energetycznych bez potrzeby wstrzymywania ruchu, a Straż Graniczna – do obserwacji pasów granicznych i wykrywania przemytu. Korzystają z nich także służby miejskie, ochrony środowiska i wiele innych. Polska odgrywa również istotną rolę w produkcji BSP – Grupa WB, jeden z największych producentów w Europie, dostarczy Wojsku Polskiemu 10 tys. dronów Warmate (kontrakt podpisano 15 maja 2025 r.). To bardzo nowoczesny sprzęt bojowy, te tzw. drony mogą działać autonomicznie, przenoszone przez jednego żołnierza lub integrowane z pojazdami, a ich systemy automatyzujące lot i naprowadzanie pozwalają na precyzyjne uderzenia w wyznaczone cele.

Zebrane w raporcie dane i przykłady pokazują, że Polska – mimo wielu opóźnień i niedostatków, o których nie wspominałyśmy – konsekwentnie buduje wielowarstwowy, zintegrowany system bezpieczeństwa obejmujący kluczowe obszary transportu i ochrony granic. Rozwój inteligentnych systemów zarządzania ruchem, cyfrowa modernizacja kolei oraz wdrożenie kompleksowego nadzoru perymetrycznego na granicach znacząco zwiększają zdolność państwa do przeciwdziałania zagrożeniom i reagowania na incydenty w czasie rzeczywistym. Szczególną rolę w tej transformacji odgrywają bezzałogowe statki powietrzne, które nie tylko wspierają operacyjnie służby, ale też stają się symbolem nowego podejścia do bezpieczeństwa – szybkiego, elastycznego i skalowalnego. Kolejne lata pokażą, w jakim stopniu te technologie zostaną skutecznie wkomponowane w struktury administracji publicznej, obronności i zarządzania kryzysowego – i czy tempo ich wdrażania nadąży za dynamiką współczesnych zagrożeń. •



Ilustracje: Marta Kołodziejak



Bezpieczna granica

od prostych rozwiązań po zaawansowane systemy

Czym innym dobrosąsiedzkie stosunki, a czym innym to, że w swoich progach chcemy gościć tylko tych, których zapraszamy. Pod tym względem podejście zwykłego Kowalskiego nie różni się od podejścia ogólnokrajowego. Chcemy mieć pewność, że tak jak nasze domy, tak i nasze granice są nienaruszalne, i w swoim domu możemy się czuć bezpiecznie. Jak fizycznie chronione są granice?

Monika Żuber-Mamak

P

Polska graniczy z siedmioma państwami: Niemcami na zachodzie (467 km na lądzie i 22 km na wodach terytorialnych), Czechami na południowym zachodzie (796 km), Słowacją na południu (541 km), Ukrainą na południowym wschodzie (535 km), Białorusią na wschodzie (418 km), Litwą na północnym wschodzie (104 km) oraz z Rosją (210 km na lądzie i ok. 22 km na wodach terytorialnych). Od północy mamy jeszcze dostęp do Morza Bałtyckiego (linia brzegowa ma ok. 770 km), choć nie graniczymy na Bałtyku bezpośrednio z żadnym państwem. Całkowita długość granic lądowych wynosi zatem 3071 km. Od kiedy jesteśmy w strefie Schengen, ochronie bezpośredniej podlegają tylko trzy graniczne odcinki – z Białorusią, Ukrainą i Rosją. Razem 1163 km granicy, która wymaga szczególnego nadzoru.



Siedmiu sąsiadów, ale tylko trzy granice

Polska weszła do strefy Schengen 21 grudnia 2007 r., co oznaczało zniesienie kontroli granicznych na granicach lądowych i morskich z innymi państwami należącymi do tego obszaru. 30 marca 2008 r. zniesiono również kontrole na lotniskach. Strefa Schengen to obszar obejmujący większość krajów Unii Europejskiej oraz kilka państw spoza niej, gdzie podróżni mogą przemieszczać się swobodnie bez konieczności przechodzenia odpraw paszportowych na granicach wewnętrznych. Wejście Polski do strefy umożliwiło nam swobodne podróżowanie na podstawie dowodu osobistego, a także zapewniło Polsce dostęp do Systemu Informacyjnego Schengen (SIS), służącego do wymiany danych o osobach

poszukiwanych czy nielegalnie przebywających. W zamian Polska podjęła zobowiązanie do ochrony zewnętrznych granic Unii Europejskiej, w tym granic z Ukrainą, Białorusią i Rosją.

Ukraina

Granica polsko-ukraińska, licząca około 535 km, stanowi nie tylko istotny odcinek lądowej granicy Polski, lecz także ważną część zewnętrznej granicy Unii Europejskiej i strefy Schengen. Ochronę tego obszaru zapewnia przede wszystkim Straż Graniczna, której działania koordynują m.in. Bieszczadzki i Nadbużański Oddział. Na tym odcinku funkcjonuje kilka kluczowych przejść granicznych – między innymi w Dorohusku, Hrebennem, Medyce, Korczowej i Zosinie – gdzie prowadzone są kontrole zarówno paszportowe, jak i celne. W ramach codziennego nadzoru granica jest patrolowana pieszo, konno, pojazdami oraz z użyciem dronów i psów tropiących. W terenie rozmieszczone są kamery, czujniki ruchu, wieże obserwacyjne i systemy termowizyjne. Polska współpracuje także z ukraińskimi służbami granicznymi oraz unijną agencją Frontex. Granica ta mierzy się z licznymi wyzwaniami, w tym z próbami nielegalnego przekraczania, przemytem oraz konsekwencjami wojny w Ukrainie, które spowodowały wzmożony ruch uchodźców. W związku z tym prowadzone są intensywne inwestycje w infrastrukturę i technologie ochrony, mające na celu stworzenie tzw. cyfrowej granicy bazującej na zintegrowanych systemach nadzoru i szybkiej wymianie informacji.

Po 2022 r. Polska znacząco zmodernizowała system ochrony granicy z Ukrainą, dostosowując go do nowych wyzwań wynikających z wojny i zwiększonego ruchu migracyjnego. Wprowadzono zaawansowane systemy elektroniczne, takie jak kamery termowizyjne, czujniki ruchu i wieże obserwacyjne, tworząc tzw. barierę elektroniczną na tych odcinkach granicy, na których było to możliwe. Przykładowo, na Podkarpaciu funkcjonuje już 32-kilometrowy odcinek takiej bariery, a w województwie lubelskim planowana jest budowa kolejnych 69 km zabezpieczeń.

W odpowiedzi na zwiększony napływ uchodźców z Ukrainy od 25 lutego 2022 r. umożliwiono przekraczanie granicy w ruchu pieszym na wszystkich drogowych przejściach granicznych z Ukrainą. Dodatkowo wprowadzono elektroniczny dokument pobytowy Diia.pl, który umożliwia obywatelom Ukrainy legalny pobyt w Polsce oraz swobodne przemieszczanie się w ramach strefy Schengen. Wzrosły również inwestycje w infrastrukturę graniczną. W 2022 r. przeznaczono ponad 11,5 mln euro na modernizację przejść granicznych na granicy polsko-ukraińskiej. Straż Graniczna planuje dalsze inwestycje, w tym budowę systemów perymetrycznych oraz modernizację bazy szkoleniowej, co łącznie wyceniono na blisko 3 mld zł.

Te działania mają na celu nie tylko zwiększenie bezpieczeństwa, ale także usprawnienie odpraw granicznych i dostosowanie infrastruktury do obecnych realiów geopolitycznych.

Rosja

Granica Polski z obwodem kaliningradzkim Federacji Rosyjskiej, licząca około 210 km, stanowi strategicznie ważny odcinek zewnętrznej granicy Unii Europejskiej. Prawie 200 km to granica lądowa, a reszta biegnie przez Zalew Wiślany i Zalew Kuroński. Po 2022 r. – w kontekście wojny Rosji z Ukrainą i wzrostu zagrożeń hybrydowych – Polska znacząco wzmocniła ochronę tego



odcinka, reagując na rosnące zagrożenia hybrydowe i możliwość wykorzystania migracji jako narzędzia presji politycznej. Zamiast trwałego muru zastosowano tymczasową zaporę z trzech rzędów drutu ostrzowego typu concertina, która do marca 2023 r. objęła ponad 100 km lądowego odcinka granicy. Równocześnie rozpoczęto budowę nowoczesnej bariery elektronicznej, obejmującej cały przebieg granicy z Rosją. System ten składa się z sieci kamer dzień-nocnych, urządzeń termowizyjnych, czujników ruchu i kabli detekcyjnych, zintegrowanych z centrum nadzoru w Kętrzynie. Granica została całkowicie zamknięta dla ruchu – zarówno osobowego, jak i towarowego – a przejścia graniczne, takie jak Bezledy czy Gronowo, pozostają nieczynne. Działania te mają na celu skuteczne wykrywanie wszelkich prób naruszania terytorium Polski oraz przeciwdziałanie zagrożeniom wywiadowczym i destabilizującym.

Białoruś

Granica polsko-białoruska, o długości około 418 kilometrów, jest jednym z najważniejszych i jednocześnie najbardziej chronionych odcinków zewnętrznej granicy Unii Europejskiej. Jest to granica lądowa, która biegnie wzdłuż granic administracyjnych województw podlaskiego i lubelskiego. Ochroną tego terenu zajmuje się przede wszystkim Straż Graniczna, wspierana przez policję oraz Wojska Obrony Terytorialnej. Fizyczna ochrona granicy państwa to proste mechaniczne zapory połączone z zaawansowanymi systemami inżynieryjnymi i elektroniką. Od stalowych szlabanów po betonowe „gwiazdy” – *dragon's teeth*. Wszystko po to, by uniemożliwić nielegalne przekroczenie granicy. W odpowiedzi na rosnące zagrożenia hybrydowe, szczególnie nasilone od 2021 r., Polska zdecydowała się na budowę trwałej zapor fizycznej.

Zapora ta składa się z wysokiego na 5,5 m ogrodzenia z siatki stalowej oraz z drutu kolczastego na górze, co ma skutecznie uniemożliwiać nielegalne przekroczenia granicy. Dodatkowo wzdłuż granicy zainstalowano system elektroniczny, obejmujący 206 km, wyposażony w kamery dzień-nocne, termowizyjne oraz czujniki ruchu, co stanowi istotne wzmocnienie monitoringu granicy. Koszt całej inwestycji wyniósł około 1,6 mld zł. W ramach działań zabezpieczających wprowadzono również strefę buforową wzdłuż granicy, obejmującą m.in. powiaty hajnowski i białostocki, mającą

”

Dane Straży Granicznej pokazują zmienną skuteczność polskiej bariery: w 2021 r., przed jej ukończeniem, odnotowano około 39 700 prób nielegalnego przekroczenia granicy polsko-białoruskiej. W 2022 r. liczba ta spadła do około 15 700, by następnie wzrosnąć do 22 500 w 2023 r. mimo istniejącej już bariery. Pierwszy kwartał 2024 r. przyniósł już ponad 8 tys. prób.

na celu dodatkowe zabezpieczenie przed nielegalnym przekroczeniem granicy. Ponadto w rejonie rzek granicznych, takich jak Bug, Świsłocz czy Istocznica, realizowane są projekty budowy dodatkowych barier elektronicznych, których koszt szacowany jest na ponad 364 mln zł.

Mój dom moim zamkiem

Właściciele prywatnych nieruchomości chronią je za pomocą płotków, murów, siatek ogrodzeniowych. Państwo, strzegąc swoich granic, sięga po podobne przeszkody, choć na większą skalę. Na własnym podwórku chcemy się czuć bezpiecznie.

Różnego rodzaju mechaniczne zapory uniemożliwiające przekroczenie granicy państwa są stosunkowo prostymi sposobami jej ochrony. Nie zawsze to, co skuteczne, musi być przecież skomplikowane. A w połączeniu z zaawansowaną elektroniką fizyczne bariery są naprawdę trudne do pokonania. Klasyczne szlabany, bramki obrotowe dla pieszych czy wysuwane z jezdni kolczatki – wszystkie te rozwiązania służą jednemu celowi: umożliwić służbom granicznym precyzyjną kontrolę ruchu transgranicznego.

Na newralgicznych odcinkach granic, szczególnie tych narażonych na próby forsowania pojazdami, coraz częściej instalowane są tzw. **smocze zęby (*dragon's teeth*)** – masywne betonowe lub stalowe bloki o wysokości od pół do półtora metra, rozmieszczone w geometrycznych wzorach. Te konstrukcje, pierwotnie projektowane jako przeszkody przeciwczołgowe podczas II wojny światowej, dziś służą jako **skuteczna bariera** przeciw nielegalnym przejazdom.



Niby proste, a przecież skuteczne. W punktach kontrolnych na przejściach granicznych są niezastąpione. Co nie zmienia faktu, że arsenał środków bezpieczeństwa granicznego jest dzisiaj bardziej rozbudowany niż kiedykolwiek wcześniej.

Kiedy potrzebne jest szybkie zabezpieczenie granicy, służby sięgają po rozwiązania tymczasowe. Zapory modułowe – prefabrykowane elementy, które można łatwo transportować i montować – oraz gabiony – kosze z siatki stalowej wypełnione kamieniami lub piaskiem – pozwalają na utworzenie skutecznej bariery w ciągu zaledwie kilku dni. Badania Uniwersytetu w Tel Awiwie dowodzą, że takie tymczasowe zabezpieczenia, gdy są prawidłowo zainstalowane i monitorowane, zmniejszają liczbę nielegalnych przekroczeń granicy o 56-72%.

Współczesna ochrona granicy to jednak znacznie więcej niż fizyczne bariery. Nowoczesne systemy monitoringu – kamery termowizyjne o zasięgu do 20 km, radary naziemne, drony patrolowe czy zaawansowane systemy analityki obrazu wykorzystujące sztuczną inteligencję – tworzą niewidzialną, lecz niezwykle skuteczną warstwę ochrony.

Badania i raporty z różnych źródeł potwierdzają, że połączenie tradycyjnych struktur fizycznych (murów, ogrodzeń, zapór) z zaawansowanymi systemami elektronicznego nadzoru znacząco poprawia efektywność ochrony granicy nawet o 60–90 % w porównaniu do stosowania samych barier fizycznych. Wdrożenie sensorów sejsmicznych, radarów mikrofalowych, kamer termowizyjnych, dronów patrolowych oraz analityki opartej na sztucznej inteligencji umożliwia wcześniejsze wykrycie prób nielegalnego przekroczenia, szybszą reakcję służb i lepsze pokrycie trudno dostępnych odcinków granicy.

W marcu tego roku Donald Tusk powiedział: *Osiągnęliśmy 98% skuteczności w zatrzymywaniu nielegalnych prób przekroczenia granicy. To wszystko dzięki zdeterminowanej postawie 11 tysięcy funkcjonariuszy, którzy stacjonują na naszej wschodniej granicy. Każdy, kto ułatwia nielegalne przekraczanie granicy, uderza w nasze bezpieczeństwo. Dlatego nasi funkcjonariusze będą działać w sposób zdecydowany i twardy.* (Gov.pl, minister Tomasz Siemoniak o sytuacji na granicy z Białorusią, data pub.: 22.03.2025).

A jednocześnie według wielu ekspertów bariera jest najbardziej skuteczna w ograniczaniu prób przekraczania granicy przez małe grupy osób i pojedyncze osoby, natomiast jej efektywność spada w przypadku zorganizowanych grup wyposażonych w profesjonalny sprzęt.

Nasza własna tarcza

Tarcza Wschód to pięcioletni (2024–2028) program obronny Polski, który obejmuje wzmocnienie ochrony wschodniej granicy kraju. Jego celem jest budowa i modernizacja różnego rodzaju przeszkód inżynierskich (stalowe ogrodzenia z drutem kolczastym, betonowe „smoczę zęby”, rowy przeciwpancerne), a także rozbudowę infrastruktury: punktów kontrolnych, schronów oraz centrów dowodzenia. W projekcie przewidziano instalację zaawansowanych systemów monitoringu: kamery dzień-noc, czujniki ruchu, termowizję i drony, które mają wspierać Straż Graniczną, Wojska Obrony Terytorialnej i inne służby. Program to skutek kryzysu migracyjnego na granicy polsko-białoruskiej w 2021 r., a także reakcja na inwazję Rosji na Ukrainę od początku 2022 r. Z punktu widzenia władz państwowych Tarcza Wschód ma

Bariera fizyczna i elektroniczna znacząco utrudniła nielegalne przekraczanie granicy i zwiększyła skuteczność działań Straży Granicznej, jednak nie wyeliminowała całkowicie tego. Z danych Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA) oraz Straży Granicznej wynika, że:

- **SKUTECZNOŚĆ:** Szef rządu w marcu 2025 r. poinformował, że udaje się powstrzymać aż **98% prób nielegalnego przekroczenia granicy**.

- **SPADEK PRÓB:** Po wprowadzeniu strefy buforowej (od 13 czerwca 2024 r. do 6 marca 2025 r.) liczba prób nielegalnego przekroczenia granicy polsko-białoruskiej spadła o około **46%** w porównaniu do analogicznego okresu przed wprowadzeniem strefy (z blisko 23,5 tys. do ponad 12,7 tys.).

- **WZMOCNIENIE I MODERNIZACJA:** Bariera fizyczna (stalowa konstrukcja o wysokości 5,5 m i długości 186 km) została zmodernizowana, m.in. poprzez wzmocnienie poziomymi stężeniami i dodatkowym zwojem drutu ostrzowego. Bariera elektroniczna (206 km) również została zmodernizowana, w tym montaż dodatkowych kamer, oświetlenia LED i wykorzystanie sztucznej inteligencji do klasyfikacji alarmów.

- **UŁATWIENIE PRACY SŁUŻB:** Bariera elektroniczna, składająca się z czujników ruchu i kamer, zapewnia monitoring wszystkich zdarzeń na linii granicy, co pozwala na szybszą reakcję patroli Straży Granicznej.

Mimo barier, migranci nadal podejmują próby przekroczenia granicy, stosując nowe metody, np. wycinanie profili zapory przy użyciu szlifierek akumulatorowych, pił i palników. Wciąż dochodzi również do ataków na funkcjonariuszy i żołnierzy na granicy. W 2024 r. odnotowano blisko 30 tys. prób nielegalnego przekroczenia granicy, z czego najwięcej (ponad 7 tys.) w maju ub.r. Bilans ostatniego majowego weekendu tego roku to ponad 400 prób nielegalnego przekroczenia granicy.



przede wszystkim odstraszać i zapewniać lepszą kontrolę i szybszą reakcję służb na incydenty graniczne. Ministerstwo Obrony podkreśla, że celem projektu jest **zabezpieczenie wschodniej flanki NATO i UE** – w praktyce wzmocnienie „ściany wschodniej” Polski – i przeciwdziałanie zagrożeniom ze strony Rosji i Białorusi. Realizując to, Tarcza Wschód ma:

- zwiększyć odporność państwa na ataki i wojnę hybrydową, **odstraszać przeciwnika** oraz ograniczać jego mobilność przy jednoczesnym zapewnieniu mobilności własnych wojsk;
- budować rozległy **system fortyfikacji i przeszkód inżynierskich**, korzystając także z naturalnych walorów terenu (bagna, lasy itp.), tak aby utrudnić przenikanie wojsk w głąb kraju;
- zwiększyć **bezpieczeństwo żołnierzy i ludności cywilnej** – np. poprzez budowę schronów, wzmocnienie indywidualnego wyposażenia, systemów monitoringu i łączności;
- skoordynować obronę granicy z działaniami sojuszników – MON zapowiada współpracę z krajami bałtyckimi i NATO (m.in. „Bałtycką Linią Obrony”) oraz możliwość częściowego finansowania inwestycji ze środków unijnych i funduszy bezpieczeństwa.

Program został formalnie ustanowiony uchwałą Rady Ministrów z czerwca 2024 r., z budżetem ok. 10 mld zł na lata 2024–2028. Minister Obrony oraz wiceministrowie podkreślają, że Tarcza Wschód to „największy od II wojny projekt” obronny w Europie Zachodniej. Jak wyjaśnia MON, to przedsięwzięcie wielodyscyplinarne – angażujące wojsko, MSWiA, samorządy – mające na celu „przygotowanie terenów przygranicznych do obrony” oraz stworzenie trwałej zapy militarnej przy granicy.

Podkreślany przez rząd **kontekst bezpieczeństwa** bezpośrednio wiąże się z ostatnimi kryzysami: prowokacją migracyjną na granicy z Białorusią w 2021 r. oraz wojną Rosji przeciwko Ukrainie od 2022 r. Polskie władze uznały te zdarzenia za elementy hybrydowego nacisku. Działania Łukaszenki, sprowadzającego migrantów na wschodnią granicę UE, określano w dokumentach jako użycie ludzi „jako broń” przeciw Polsce. Polski chargé d'affaires stwierdził wręcz, że reżim białoruski „importuje ludzi, aby najechali terytorium Polski” – i w odpowiedzi na te zagrożenia buduje „barierę” oraz załączki Tarczy Wschód. Od początku kryzysu (lato 2021) Straż Graniczna i wojsko wzmocniały już istniejącą zaporę (m.in. poprzecznymi belkami, concertiną, sensorami).

Inwazja Rosji w lutym 2022 r. uświadamia, że wojna konwencjonalna na dużą skalę jest realnym zagrożeniem. Polska intensywnie zwiększyła liczebność żołnierzy na wschodniej granicy (o tysiąc osób w 2023 r.) i przyspieszyła zakupy sprzętu (opancerzone transportery, drony, systemy rozpoznania satelitarnego). W obliczu agresji Rosji MON argumentuje, że Tarcza Wschód to kontynuacja ukraińskich doświadczeń – przygotowanie terenu poprzez umocnienia i lokalne rezerwy, aby przeciwdziałać zajęciu terytorium. Program odwołuje się więc zarówno do sytuacji migrantów na granicy, jak i realnego zagrożenia militarną eskalacją z kierunku wschodniego. Jak podsumowuje MON, celem jest „ochrona terytorium Polski przed najazdem z Rosji i Białorusi”.

W dyskusjach eksperckich program Tarcza Wschód jest traktowany przede wszystkim jako projekt odstraszenia militarnego i wzmacniania obronności. Po pierwsze – ma odstraszać. Jeżeli





dojdzie do agresji Białorusi czy Rosji, będziemy lepiej przygotowani. Po drugie, ma demotywować przeciwnika (poprzez budowę pasów umocnień i przeszkód), a w razie konfliktu „spowolnić działania potencjalnego najeźdźcy”.

Tarcza Wschód jest zatem odpowiedzią na presję migracyjną i niestabilną sytuację geopolityczną. Ma przywrócić trwałą kontrolę nad wschodnią granicą Polski (i flanki NATO) oraz zwiększyć bezpieczeństwo obywateli. Niezależni analitycy zaznaczają jednak, że część uzasadnień ma wymiar polityczny (budowanie poczucia bezpieczeństwa i odstraszanie), a rzeczywisty efekt militarny będzie zależał od konkretnych rozwiązań technicznych i dalszej współpracy z sojusznikami.

Barieri fizyczne na granicach państwowych nie są zjawiskiem nowym, ale w ostatnich dekadach obserwujemy wyraźny wzrost ich liczby i stosowanie coraz bardziej zaawansowanych rozwiązań technicznych. Przed upadkiem Muru Berlińskiego w 1989 r. na świecie istniało od 6 do 12 znaczących fizycznych barier granicznych. Obecnie (stan na 2022-2024) liczba ta wzrosła do co najmniej 63, 74 lub 77 murów granicznych. Liczby są różne, zależy od tego, jak liczący definiują taką graniczną zaporę lub mur. Najbardziej uderzającym wnioskiem jest zatem dramatyczny wzrost liczby fizycznych barier granicznych na świecie – niemal dziesięciokrotny od zakończenia zimnej wojny. Oznacza to, że choć wszyscy chętnie mówią o globalnej wiosce, to w tejże wiosce ceni się płoty i miedze. Zamiast więc zaniku granic obserwujemy ich ponowne umacnianie.

Badania przeprowadzone przez Stanford Immigration Policy Lab wskazują na interesującą zależność: bariery fizyczne często nie tyle powstrzymują migrację, ile przekierowują ją na inne trasy lub zmieniają jej charakter – z indywidualnej na zorganizowaną, z wykorzystaniem profesjonalnych przemytników.

23



FLIR SCOUT PRO™

TAKTYCZNY I NIEZAWODNY

Taktyczny i intuicyjny monokular termowizyjny zaprojektowany do wsparcia działań służb mundurowych i operacyjnych w terenach otwartych.

Niezawodny i niezastąpiony podczas akcji poszukiwawczo-ratowniczych oraz dotyczących bezpieczeństwa publicznego.



Daleki
zasięg



Solidna
konstrukcja



Prosta
obsługa



WWW.LINC.PL



OFICJALNY DYSTRYBUTOR:

Linc Polska Sp. z o.o.
ul. Czarnkowska 22, 60-415 Poznań
tel.: +48 61 839 19 00



Linc
Polska Sp. z o.o.



Bezpieczne miasto jest dobrze pomyślane

Bezpieczeństwo w miastach to nie tylko kwestia policyjnych patroli czy sprawnego systemu ratunkowego. To złożony ekosystem technologii, infrastruktury i projektowania przestrzeni publicznej, który ma na celu ochronę mieszkańców oraz zapewnienie im komfortu i spokoju.

Monika Żuber-Mamak



Współczesne miasta inwestują w różnorodne rozwiązania, od zaawansowanych systemów elektronicznych po fizyczne bariery i elementy małej architektury, które razem tworzą spójną strategię bezpieczeństwa.

Poczucie bezpieczeństwa w Polsce – dane i koszty

W Polsce poczucie bezpieczeństwa fizycznego pozostaje na relatywnie wysokim poziomie. W kwietniu 2024 r. aż 88% badanych przez CBOS uznało, że Polska jest krajem, w którym żyje się bezpiecznie, przy jedynie 9% przeciwnych ocen i 3% niezdecydowanych. Jeszcze bardziej optymistycznie wyglądają deklaracje dotyczące najbliższego otoczenia – według tych samych badań niemal 96% Polaków ocenia swoją dzielnicę czy osiedle jako miejsce bezpieczne i spokojne.

Nieco więcej niż co trzeci badany (36%, spadek o 4 punkty procentowe względem 2022 r.) obawia się jednak, że może stać się ofiarą przestępstwa, w tym tylko 3% boi się tego bardzo. Drugie Ogólnopolskie Badanie Wiktyimizacyjne z 2024 r. wskazuje, że w ciągu pięciu ostatnich lat 15% badanych padło ofiarą przestępstwa, co pokazuje, że pewien poziom obaw jest uzasadniony.

Niestabilne poczucie bezpieczeństwa niesie ze sobą realne koszty. W 2019 r. przestępczość obciążała budżet państwa kwotą około 5 mld zł rocznie, z czego połowa to skutki przestępstw gospodarczych. W 2025 r. może to być kwota wyższa ze względu na inflację. Nic dziwnego, że firmy i gospodarstwa domowe coraz częściej inwestują w prywatne systemy ochrony, monitoring i polisy ubezpieczeniowe, aby zrekompensować niedostatki bezpieczeństwa publicznego.

Biorąc powyższe pod uwagę, obserwujemy interesujące zjawisko społeczne – Polacy wykazują znaczącą gotowość do rezygnacji z części prywatności w zamian za zwiększone poczucie bezpieczeństwa. Aż 43% obywateli akceptuje monitoring w przestrzeni publicznej jako efektywny sposób poprawy bezpieczeństwa mimo potencjalnego naruszania prywatności.

Urbanizacja i jej wpływ na bezpieczeństwo

Przez ostatnie dziesięciolecie w Polsce widoczny jest wyraźny trend przemieszczania się mieszkańców z obszarów wiejskich do ośrodków miejskich. Udział populacji zamieszkującej teren wiejski stopniowo się zmniejsza. Dane Głównego Urzędu Statystycznego pokazują, że w 1950 r. około 65% społeczeństwa polskiego mieszkało na wsi. W następnych dekadach proporcja ta systematycznie spadała – w 2000 r. ludność wiejska stanowiła 42% ogółu mieszkańców, w 2010 r. odsetek ten wyniósł 39,7%, a w 2021 r. zmniejszył się do 37,8%.

Tendencja ta wyraźnie wskazuje na rosnącą skłonność do osiedlania się w ośrodkach miejskich, co wynika głównie z różnic w poziomie rozwoju pomiędzy dużymi miastami a terenami wiejskimi oraz małymi miejscowościami. Obecnie prawie 61% naszych rodaków mieszka w mieście i oczekuje, że będzie to miejsce czyste, bezpieczne i z dobrze działającym transportem publicznym.

Tymczasem współczesne aglomeracje muszą mierzyć się z szeregiem złożonych wyzwań. Obejmują one zapobieganie dewastacji mienia, poprawę komunikacji i ograniczenie korków na trasach wlotowych do miasta. Poczucie bezpieczeństwa jest odczuciem głęboko indywidualnym, zależnym od wielu czynników, w tym od miejsca zamieszkania.

Różnica w percepcji bezpieczeństwa wynika z faktu, że w dużych aglomeracjach relacje międzyludzkie są często rozluźnione, a poczucie anonimowości większe. To ma swoje zalety, ale i wady. Łatwiej o chuligański wybryk, gdy jest się anonimowym. W efekcie, choć urbanizacja przynosi korzyści ekonomiczne i rozwój, nieuchronnie osłabia spójność społeczną i zwiększa anonimowość, co bezpośrednio koreluje z niższym subiektywnym poczuciem bezpieczeństwa i potencjalnie wyższymi wskaźnikami przestępczości.

Kluczowym elementem w budowaniu bezpiecznej przestrzeni miejskiej jest jej prawidłowe zaprojektowanie. Uwzględnienie takich elementów miejskiej infrastruktury, które z jednej strony ułatwią życie mieszkańcom, z drugiej nie odbiorą im prywatności, a z trzeciej nie zamienią miejskiej przestrzeni w więzienny spaceriak.

Monitoring miejski – technologia na straży bezpieczeństwa

Monitoring wizyjny jest jednym z najskuteczniejszych rozwiązań w zakresie ochrony osób i mienia w miastach. Umożliwia nadzór za pomocą kamer dozorowych (CCTV), których obrazy są przesyłane do bazy danych, zazwyczaj połączonej z centrum zarządzania. Dzięki temu możliwy jest bieżący podgląd tego, co dzieje się w monitorowanych lokalizacjach, a rejestrowane obrazy są zapisywane i archiwizowane.

Nowoczesne urządzenia są bardzo czułe, rejestrują obraz nawet przy słabym oświetleniu, a większość sprawnie działa również w ciemności, niezależnie od złej pogody. Monitoring miejski



często działa jako część zintegrowanego systemu bezpieczeństwa, ułatwiając działania prewencyjne służb porządkowych, wspomagając zarządzanie transportem miejskim, a nawet będąc częścią systemu przeciwpożarowego z wykorzystaniem kamer termowizyjnych.

Obecność kamer skutecznie odstrasza przestępców, zmniejszając skłonność do popełniania wykroczeń, a w przypadku zdarzeń (wypadków, pożarów, kradzieży) umożliwia szybkie podjęcie działań i dostarcza dowodów niezbędnych do ujęcia sprawców.

Warto zauważyć, że przyszłość monitoringu miejskiego to nie tylko obserwacja zdarzeń, ale przewidywanie potencjalnych incydentów i interwencja, zanim sytuacja eskaluje. Systemy zabezpieczeń wyposażone w algorytmy uczenia maszynowego mogą automatycznie analizować dane z kamer, czujników i innych urządzeń, co pozwala na wczesne wykrywanie podejrzanych aktywności.

Ta zmiana paradygmatu – od zbierania dowodów po fakcie do proaktywnego, opartego na sztucznej inteligencji wykrywania zagrożeń – przekształca centra monitoringu w ośrodki analityki predykcyjnej, co może prowadzić do znacznego zmniejszenia przestępczości i szybszego reagowania służb ratunkowych.

Fizyczne systemy bezpieczeństwa

Fizyczne systemy zabezpieczeń stanowią namacalną warstwę ochrony w przestrzeni miejskiej, uzupełniając rozwiązania elektroniczne i zapewniając ochronę pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń, takich jak pożar, powódź, kradzież, wandalizm czy terroryzm.

Blokady drogowe, szlabany i wysuwane słupki

Wśród fizycznych systemów zabezpieczeń kluczową rolę odgrywają blokady drogowe, szlabany i wysuwane słupki. Słupki parkingowe i drogowe, dostępne w wersjach automatycznych, ręcznych, składanych i wysuwanych, stanowią elastyczną alternatywę dla tradycyjnych szlabanów. Pozwalają one na swobodny ruch pieszy i rowerowy, jednocześnie skutecznie blokując ruch samochodowy.

Są stosowane do zabezpieczania wjazdów na place, deptaki, ulice czasowo udostępniane dla ruchu, a także do wygradzania indywidualnych miejsc parkingowych na parkingach osiedlowych czy w garażach podziemnych. Słupki automatyczne mogą być sterowane pilotem, kartą magnetyczną lub SMS-em, co zapewnia pełen komfort użytkowania i elastyczność zarządzania.

Bariery antyterrorystyczne i elementy architektury miejskiej

W obliczu rosnących zagrożeń terrorystycznych, zwłaszcza ataków z wykorzystaniem pojazdów, miasta coraz częściej wdrażają zaawansowane bariery antyterrorystyczne. Słupki antyterrorystyczne, tzw. bollardy, są projektowane tak, aby wytrzymać uderzenie ciężarówki. Na przykład bollard w klasie M30 (K4) wytrzyma uderzenie pojazdu ciężarowego o masie 7,5 tony, jadącego z prędkością 80 km/h.

Bollardy mogą być opuszczane i podnoszone w ciągu 4-6 sekund (a nawet 1,5 sekundy z systemem EFO) za pomocą pilota, sterownika radiowego lub modułu GSM, co pozwala na



kontrolowany wjazd pojazdów uprzywilejowanych do chronionych stref.

Poza tradycyjnymi słupkami coraz częściej wykorzystuje się elementy architektury miejskiej, takie jak ławki, donice, kosze na śmieci czy stojaki rowerowe, które są projektowane jako zapory krajobrazowe. Przykładem może być Poznań, gdzie w 2019 r. zainstalowano 12 betonowych ławek, z których każda waży 800 kg. Oficjalnie mają one służyć jako zabezpieczenie przed niespodziewanym wjazdem pojazdu w tłum ludzi podczas uroczystości i imprez masowych.

Jednak ich masywna konstrukcja i brak oparcia sprawiają, że są niewygodne do dłuższego siedzenia, a tym bardziej do leżania, co wpisuje się w koncepcję wrogiej architektury. Te rozwiązania mają



”

Fizyczne systemy zabezpieczeń stanowią namacalną warstwę ochrony w przestrzeni miejskiej, uzupełniając rozwiązania elektroniczne i zapewniając ochronę pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych.

na celu zniechęcenie intruzów, opóźnienie ich działań i umożliwienie reakcji na potencjalny atak lub bezpieczną ewakuację.

Adaptacja architektury miejskiej do celów bezpieczeństwa jest bezpośrednią odpowiedzią na zmieniające się zagrożenia, gdzie zatłoczone miejsca publiczne stały się głównym celem ataków terrorystycznych z użyciem pojazdów. Połączenie zabezpieczeń z tzw. meblami miejskimi oznacza, że bezpieczeństwo nie polega już tylko na widocznych barierach, ale także na subtelny komponowaniu środków ochronnych w estetyczną i funkcjonalną tkankę miasta.

Projektowanie urbanistyczne staje się zatem coraz bardziej kluczowym elementem bezpieczeństwa, wykraczając poza tradycyjne zapobieganie przestępczości w kierunku działań

antyterrorystycznych. Wymaga to od architektów i urbanistów włączania solidnych, ale jednocześnie estetycznych funkcji bezpieczeństwa już na etapie projektowania, przekształcając codzienne elementy miejskie w infrastrukturę obronną.

„Wroga architektura” – kontrowersyjna, ale skuteczna?

W przestrzeni miejskiej coraz częściej pojawiają się elementy określone mianem „architektury wrogiej” (*hostile architecture*) lub „defensywnego urbanizmu” (*defensive urbanism*). Są to celowo zaprojektowane elementy infrastruktury, których zadaniem jest ograniczenie dostępu do przestrzeni publicznej i zniechęcenie do pewnych zachowań, często skierowane przeciwko grupom marginalizowanym, takim jak osoby bezdomne.

Najczęściej spotykane przykłady:

- **Kolce i wypukłości:** metalowe kolce, guzy lub inne spiczaste struktury umieszczane na gzymsach budynków, pod zadaszeniami, wokół sklepów, a nawet na chodnikach, aby uniemożliwić siadanie, leżenie czy rozłożenie posłania.
- **Ławki zaprojektowane tak, by uniemożliwić spanie:** mogą to być ławki o pochylonym siedzisku, które wymuszają ciągłe podpieranie się stopami, ławki z podłokietnikami umieszczonymi na środku, uniemożliwiającymi położyć się, lub ławki zbyt krótkie, by na nich się położyć. Przykładem są tzw. ławki Camden w Londynie, zaprojektowane tak, by zniechęcać do spania, jazdy na deskorolce czy naklejania naklejek.
- **Inne przeszkody i bariery:** duże donice z kwiatami, głazy, ogrodzenia, kraty, nadmierna liczba stojaków rowerowych na chodnikach czy strategicznie rozmieszczone krzewy, które mają uniemożliwić koczowanie lub rozbijanie namiotów.
- **Mniej oczywiste lub bardziej agresywne metody:** sporadycznie uruchamiane zraszacze wodne, głośna muzyka odtwarzana w celu odstraszenia osób przebywających w danym miejscu czy specjalne powierzchnie odchylające mocz, by trafił w osobę oddającą mocz w miejscu publicznym.

Oficjalnym celem tych rozwiązań jest często poprawa bezpieczeństwa, estetyki lub porządku publicznego. Jednak krytycy wskazują, że „wroga architektura” nie rozwiązuje problemu bezdomności, lecz jedynie spycha osoby bezdomne z widoku, często z dala od usług społecznych.

W Polsce tego typu rozwiązania są również stosowane, choć w subtelniejszej formie. Przykładem są ławki z dodatkowymi metalowymi barierkami uniemożliwiającymi leżenie, co budzi kontrowersje, szczególnie w kontekście osób bezdomnych. Ich wprowadzenie spotkało się z krytyką w mediach społecznościowych i na forach miejskich.

Dyskutujący podnoszą słuszny argument, że takie projekty owszem utrudniają życie grupom docelowym, ale także sprawiają, że przestrzeń publiczna staje się mniej komfortowa dla wszystkich użytkowników, w tym osób starszych, niepełnosprawnych czy rodzin z dziećmi, które potrzebują miejsca do odpoczynku.

Debata na temat „wrogiej architektury” podkreśla potrzebę bardziej inkluzywnego i zrównoważonego podejścia do projektowania przestrzeni miejskiej, które równoważy kwestie bezpieczeństwa z potrzebami wszystkich mieszkańców.



Zarządzanie ruchem drogowym – woonerfy i innowacyjne rozwiązania

Bezpieczeństwo w miastach to także odpowiednie zarządzanie ruchem drogowym. Woonerfy, czyli strefy uspokojonego ruchu, oraz tzw. uszy Myszki Miki to przykłady rozwiązań urbanistycznych, które mają na celu spowolnienie ruchu pojazdów i zwiększenie bezpieczeństwa pieszych.

Koncepcja woonerfów (podwórców miejskich)

Woonerf, czyli „ulica do mieszkania” w wolnym tłumaczeniu z języka holenderskiego, to rewolucyjna idea projektowania przestrzeni miejskiej, która łączy funkcje ulicy, parkingu, promenady i miejsca spotkań mieszkańców. Kluczową zasadą jest priorytetowe traktowanie pieszych i rowerzystów przy jednoczesnym zachowaniu niezbędnej obsługi komunikacyjnej, w tym parkingowej.

Dopuszczalna prędkość pojazdów wynosi 20 km/h, a parkowanie jest możliwe tylko w wyznaczonych miejscach. Co więcej, dzieci do 7 lat mogą korzystać z drogi bez opieki, co jest wyjątkiem od ogólnych przepisów (według badania „Rozwój idei stref woonerf w Polsce na przykładzie miasta Łodzi”, Michał Betlej, Aleksandra Radziejowska, 2019 r.).

Projektowanie woonerfów opiera się na zacieraniu podziałów między jezdnią a chodnikiem oraz stosowaniu „szykan” – małych elementów architektonicznych, takich jak klomby, ławki, stojaki rowerowe czy słupki, które wymuszają zmianę toru jazdy i spowalniają ruch.

Woonerfy znacząco zwiększają przestrzeń przyjazną dla pieszych i cyklistów, redukują hałas i zanieczyszczenia, poprawiają estetykę, zwiększają ilość zieleni i sprzyjają integracji społecznej. Choć zmniejszają przepustowość dla samochodów i są droższe w realizacji i utrzymaniu, ich korzyści dla jakości życia w centrum miasta są znaczące.

Uszy Myszki Miki i inne poszerzenia chodników

To innowacyjne rozwiązanie stosowane na skrzyżowaniach, polegające na charakterystycznym poszerzeniu chodnika, którego nazwa pochodzi od jego kształtu. Uszy Myszki Miki mają za zadanie uspokoić ruch, poprawić widoczność na skrzyżowaniach i przejściach dla pieszych, a także efektywnie wykorzystać przestrzeń, umożliwiając wydzielenie dodatkowych miejsc parkingowych.

Pozyskana dzięki nim przestrzeń może być wykorzystana na zielen, stojaki rowerowe, a nawet na ogródki kawiarniane. W przypadku ulic jednokierunkowych z dopuszczonym ruchem pod prąd jednostronne „ucho” poprawia widoczność rowerzystów, sprawiając, że ich tor ruchu jest bardziej czytelny.

Progi zwalniające i szykany drogowe – skuteczność vs. wady

Progi zwalniające są poprzecznymi wypukłościami na jezdni, których celem jest ograniczanie prędkości pojazdów. Materiałem do ich wykonania jest zazwyczaj guma lub kostka betonowa, a miejsca ich instalacji są oznaczone znakiem A-11a.

Rodzaje progów zwalniających:

- „Pinezka” – okrągła wypukłość na środku skrzyżowania
- „Poduszka” – prostokątna, obejmująca jedynie środkową część skrzyżowania
- „Próg wyspowy” – tzw. *bus-friendly* zwany też „poduszką berlińska”, którego konstrukcja pozwala autobusom na płynniejszy przejazd, jednocześnie wymuszając spowolnienie ruchu samochodów osobowych

Progi są stosunkowo tanie w instalacji i skutecznie redukują prędkość lokalnie, pomagając w eliminacji ruchu tranzytowego. Mają jednak istotne wady: generują hałas i wibracje (szczególnie uciążliwe dla mieszkańców, prowadząc nawet do pęknięć ścian w budynkach), zwiększają emisję spalin (pył z klocków hamulcowych i opon), są niebezpieczne dla rowerzystów i motocyklistów, spowalniają pojazdy uprzywilejowane (ambulansy, straż pożarną, policję), negatywnie wpływają na infrastrukturę drogową i utrudniają odśnieżanie.

Bywają też zbyt wysokie, co prowadzi do uszkodzeń pojazdów. Progi cenione są przez pieszych, bo spowalniają ruch, aż do czasu gdy taki pieszy nie wsiądzie za kierownicę. Wtedy optyka się diametralnie zmienia.

Ciekawe pomysły dotyczące progów można znaleźć w artykule opublikowanym



w 2018 r. w czasopiśmie „Logistyka” (*Progi zwalniające jako element uspokajania ruchu*, Jan Targosz, Jacek Wiederek, Angelika Kozerska). Autorzy przedstawiają trzy interesujące rozwiązania:

- Próg wyposażony w centralny zawias oraz amortyzator o odpowiednio dobranych parametrach, który spłaszcza się podczas wolnej jazdy, ale zachowuje wypukły kształt przy większych prędkościach
- Próg w formie rękawa zawierającego ciecz, która rozlewa się przy powolnym najeździe pojazdu, natomiast stawia opór w przypadku szybkiego przejazdu (na zasadzie cieczy nienewtonowskiej)
- Próg z elastyczną nawierzchnią, która ugina się pod ciężarem pojazdów ciężkich takich jak autobusy, ale pozostaje stabilna podczas przejazdu samochodów osobowych

Rozwiązania te wydają się jednak w dalszym ciągu pozostawać w sferze koncepcji.

Szykany drogowe – subtelniejsze podejście

Szykany drogowe są fizycznymi elementami infrastruktury, które w bardziej subtelny sposób wymuszają redukcję prędkości poprzez odpowiednie zawężenie pasa ruchu lub zmianę jego przebiegu. Mogą przybierać różne formy:

- **Szykany esowe** – odgięcie toru jazdy
- **Naprzemienne** – wysepki, donice z roślinnością
- **Podwójne** – zwężenie drogi dla jednego pojazdu
- **Z wyspami azylu** – stosowane przy przejściach dla pieszych, zapewniające bezpieczeństwo pieszym i zmuszające kierowców do ograniczenia prędkości
- **Z powierzchnią spowalniającą**

Ich skuteczność zależy od odpowiedniego rozmieszczenia i różnorodności zastosowanych rozwiązań, często w połączeniu z wyniesionymi przejściami dla pieszych czy azylami. Szykany poprawiają bezpieczeństwo, zwiększają płynność ruchu (zapobiegając gwałtownym hamowaniom i przyspieszeniom), redukują hałas i emisję spalin, a także mogą poprawiać estetykę przestrzeni miejskiej.

W strefach „tempo 30” są uzupełniane przez skrzyżowania równorzędne, wyniesione tarcze skrzyżowań i bramy wjazdowe, które jasno sygnalizują zmianę warunków ruchu. Na trasach autobusowych stosuje się rozwiązania, takie jak centralne wyspy czy lokalne poszerzenia chodników, aby zapewnić płynność komunikacji miejskiej. Spowolnienie ruchu miejskiego wykracza poza zwykłe fizyczne przeszkody, zmierzając w kierunku bardziej wyrafinowanego podejścia zakorzenionego w psychologii behawioralnej i zintegrowanym projektowaniu urbanistycznym. Progi zwalniające, choć skuteczne w wymuszaniu redukcji prędkości, generują liczne negatywne skutki uboczne. W przeciwieństwie

do nich woonerfy i szykany, poprzez zacieranie podziałów między jezdnią a chodnikiem, wymuszanie zmiany toru jazdy i sprawiając, że ulice stają się „mniej przyjemnymi i potencjalnie niebezpiecznymi” dla kierowców, subtelnie wpływają na ich zachowanie i percepcję. Celem jest nie tylko spowolnienie samochodów, ale także stworzenie wspólnej, wielofunkcyjnej przestrzeni, w której wszyscy użytkownicy odczuwają odpowiedzialność i naturalnie dostosowują swoje zachowanie, zamiast być zmuszani przez bariery fizyczne.

Bezpieczeństwo w miastach jest złożonym zagadnieniem, które wymaga wielowymiarowego podejścia, łączącego zaawansowane technologie, fizyczne bariery, przemyślane projektowanie przestrzeni publicznej oraz świadomą politykę społeczną. Rozwój inteligentnych miast (*Smart City*) i technologii Internetu rzeczy (IoT) oferuje bezprecedensowe możliwości w zakresie monitorowania przestrzeni, zarządzania ruchem i kontroli dostępu, co przekłada się na realne zwiększenie bezpieczeństwa i komfortu życia mieszkańców.

Systemy monitoringu wizyjnego, inteligentne systemy transportowe czy elektroniczna kontrola dostępu stają się fundamentem nowoczesnego zarządzania bezpieczeństwem miejskim, umożliwiając szybką reakcję na zagrożenia i skuteczną prewencję.

Jednocześnie fizyczne rozwiązania, takie jak wysuwane słupki, szlabany czy innowacyjne bariery antyterrorystyczne wkomponowane w architekturę miejską, stanowią namacalną warstwę ochrony, adaptując przestrzeń do zmieniających się zagrożeń. Koncepcje woonerfów czy uszy Myszki Miki pokazują, jak projektowanie urbanistyczne może subtelnie wpływać na zachowania uczestników ruchu, tworząc przestrzenie bardziej przyjazne i bezpieczniejsze dla pieszych i rowerzystów, odchodząc od problematycznych rozwiązań, jakimi często są progi zwalniające.

Kluczowe jest znalezienie właściwej równowagi między bezpieczeństwem a dostępnością, między ochroną a włączeniem społecznym, między nowoczesnymi technologiami a ludzkimi potrzebami. Tylko takie zintegrowane podejście może zapewnić miastom rozwój w kierunku przestrzeni przyjaznych wszystkim mieszkańcom. •





Nowoczesne technologie zapewniają bezpieczeństwo na ulicach i w obiektach



Ochrona obiektów użyteczności publicznej i otwartych przestrzeni, w których przebywają ludzie, zawsze była ważna, ale obecnie stała się ważniejsza niż kiedykolwiek wcześniej. Na szczęście technologia idzie do przodu, a wraz z nią pojawiają się nowoczesne zabezpieczenia, które chronią przed różnymi rodzajami zagrożeń.

Do ochrony infrastruktury krytycznej i obiektów o znaczeniu strategicznym, ale też wszystkich miejsc publicznych, gdzie przebywają ludzie, wykorzystuje się produkty z grupy HVM (*Hostile Vehicle Mitigation*). Są to wszelkiego rodzaju urządzenia, których celem jest ochrona ludzi przed atakiem dokonanym za pomocą rozpędzonego pojazdu. Mogą to być m.in. słupki, blokady, barykady lub inne bariery, które mogą zatrzymać lub zredukować prędkość pojazdu, aby uniemożliwić mu dotarcie do celu.

Bezpieczeństwo w obiektach – odporne bramy garażowe

Ochrona obiektów to przede wszystkim ochrona wejść – czy to drzwi, czy bram garażowych. W miejscach o szczególnych potrzebach, m.in. siedzibach ważnych instytucji, alternatywą dla zwykłej bramy garażowej jest brama antywłamaniowa, kulooodporna lub odporna na wybuch.

Każdy z dostępnych na rynku modeli bram ma oficjalną klasę ochrony. Klasa ta

poświadcza właściwości odpowiednie dla danego zastosowania: ochronę przed próbą wtargnięcia do obiektu, odporność na ostrzał z użyciem broni palnej lub na ogień.

Specjalne ogrodzenia antywłamaniowe i antyterrorystyczne

Ogrodzenia antyterrorystyczne wyglądają jak typowe panele, jednak są niezwykle wytrzymałe. W razie ataku na co najmniej 3 minuty zatrzymują agresora, dzięki czemu służby zyskują czas, by zareagować. Rozwiązanie to warto zastosować nie tylko w obiektach o znaczeniu strategicznym, ale też jako zabezpieczenie terenu szkół, boisk, parków czy placów zabaw.

Słupki parkingowe stałe i automatyczne – ochrona przed atakami

Najważniejszą funkcją słupków parkingowych jest zapewnienie skutecznej kontroli dostępu do określonych obszarów. Modele automatyczne są nowoczesną alternatywą dla szlabanów.

Stale natomiast chronią przestrzeń wyłączoną z ruchu pojazdów. Sprawdzają się nie tylko na typowych parkingach, ale też na placach miejskich, gdzie odbywają się imprezy masowe, wiece czy inne spotkania. Zabezpieczają teren wokół urzędów, szpitali, szkół itp.

Specjalnym typem tych urządzeń są słupki antyterrorystyczne. Ich konstrukcja pozwala na skuteczne zatrzymanie ciężarówki rozpędzonej do 80 km/h! Inwestycja w takie rozwiązania znacznie podniesie bezpieczeństwo ludności miejskiej – ochroni przestrzeń publiczną przed atakami terrorystycznymi, najazdami ekstremistów czy nawet skutkami „zwykłych” wypadków na drodze.

Z myślą o estetyce – meble miejskie antyterrorystyczne

Alternatywą dla stałych zapór są stylowe meble miejskie, które równie skutecznie chronią przed atakami, a przy tym mają przyjazny design. Zapewniają bezpieczeństwo bez „straszenia” swoim wyglądem. Producenci oferują całe spektrum pomysłów – od zapór w kształcie kredek, idealnych do przestrzeni wokół szkół i przedszkoli, przez ławki i donice, aż po antyterrorystyczne stojaki na rowery i kosze na śmieci.

W trosce o szczególne obiekty – zapory antyterrorystyczne typu roadblocker

Niektóre obiekty, takie jak bazy wojskowe, wymagają zastosowania najwyższego poziomu zabezpieczeń. Zapewniają je zapory typu roadblocker. Większość z nich została zaprojektowana w klasie ochrony M30 – oznacza to, że taka blokada jest w stanie zatrzymać prawie 7-tonowy pojazd rozpędzony do 48 km/h. Przez odpowiednio umieszczony roadblocker nie przejedzie motocykl, a ruch pieszych jest znacząco utrudniony. W tych szczególnych obiektach jest to zdecydowaną zaletą.

Od lat zajmujemy się projektowaniem i realizacją systemów zabezpieczeń antyterrorystycznych oraz automatyki do bram. Oferujemy kompleksowe rozwiązania, w tym montaż i serwis urządzeń zabezpieczeń, dostosowane do indywidualnych potrzeb klientów. Dzięki wieloletniemu doświadczeniu zapewniamy naszym klientom skuteczną ochronę obiektów przed zagrożeniami. •



PPUH HERZ

ul. Ługi 74
05-400 Otwock
www.słupkiparkingowe.pl



Jak przeciwdziałać zagrożeniom w przestrzeni publicznej



Zapewnienie bezpieczeństwa w przestrzeniach publicznych stało się obecnie jednym z kluczowych wyzwań dla instytucji publicznych, samorządów, a także firm technologicznych. W świecie, w którym technologia rozwija się w błyskawicznym tempie, rodzi się pytanie – czy możemy ją skutecznie wykorzystać, by zwiększyć nasze bezpieczeństwo? Na ten temat rozmawiamy z **Arturem Hejdysem**, prezesem firmy C&C Partners.

W ostatnich miesiącach coraz częściej docierają do nas doniesienia o zagrożeniach w miejscach publicznych – szkołach, uczelniach, szpitalach czy urzędach. Czy możemy realnie zapobiegać takim sytuacjom dzięki nowoczesnym technologiom?

Tak, zdecydowanie. Dzisiejsze systemy zabezpieczeń dają nam ogromne możliwości, które, jeśli są odpowiednio wdrożone, mogą zarówno zapobiegać incydentom, jak i minimalizować ich skutki. Problemem w Polsce nie jest brak dostępnych rozwiązań, tylko zbyt wolne wdrażanie dobrych praktyk powszechnie stosowanych w innych krajach. Zagrożenia, z którymi się mierzymy, jak przebiegające na kampusach, ataki na infrastrukturę krytyczną czy działania sabotażowe, funkcjonują od dawna także w innych częściach

świata. Tam często są one objęte regulacjami, np. unijnymi dyrektywami, które określają minimalne standardy zabezpieczeń. W Polsce niestety zbyt rzadko po nie sięgamy.

Dlaczego tak się dzieje? Brakuje świadomości, wiedzy, czy może środków?

Wszystkiego po trochu. Ale największym problemem jest brak systemowego podejścia. Tymczasem jedną z naszych przewag, jako firmy technologicznej z europejskim rodowodem, jest to, że możemy bezpiecznie wymieniać się doświadczeniami z partnerami z innych krajów. Widzimy, że przeciwdziałanie zagrożeniom staje się dziś motorem postępu technologicznego. Dobrym przykładem są systemy VMS, czyli systemy zarządzania materiałem wizyjnym, które dzięki analizie i algorytmom AI potrafią wykrywać podejrzane zachowania: pojawienie się broni, pozostawiony bagaż, wejście do niedozwolonej strefy. To nie są już futurystyczne wizje, to standard w wielu wdrożeniach, również w Polsce.

Czyli system wyposażony w najnowszą technologię nie tylko „widzi”, ale i „rozumie”?

Dokładnie. Dzisiejsze systemy uczą się na bazie danych i kontekstu. Sztuczna inteligencja w systemach zabezpieczeń to już nie przyszłość – to teraźniejszość. I to nie tylko w obszarze telewizji dozorowej. Coraz powszechniej stosuje się inteligentne systemy interkomowe, wyposażone w funkcje komunikacji wielojęzycznej oraz algorytmy automatycznego udzielania pomocy. Takie systemy nie tylko umożliwiają wezwanie wsparcia, ale też są projektowane tak,

by każdy, bez względu na bariery, mógł z nich skorzystać. I co ważne: mamy takie wdrożenia już w Polsce. I znamy przypadki, kiedy takie technologie zapobiegły tragedii.

To brzmi bardzo obiecująco. Ale czy polskie instytucje są gotowe na takie rozwiązania?

Coraz bardziej. Widzimy wzrost świadomości i coraz więcej przetargów, w których nie chodzi już tylko o monitoring wizyjny, ale o kompleksowe zarządzanie bezpieczeństwem. Bo dziś nie chodzi tylko o analizę *post factum*, ale o aktywne zarządzanie sytuacją kryzysową. Zwłaszcza w sytuacjach, takich jak zagrożenia terrorystyczne, gdzie wbrew powszechnemu przekonaniu ewakuacja nie zawsze jest najlepszym rozwiązaniem. Dlatego tak ważna staje się możliwość dynamicznego przekazywania wytycznych za pomocą systemów komunikacji głosowej. Na „Zachodzie” funkcjonują w tym zakresie odpowiednie normy, my również musimy zacząć je stosować.

Z tego wynika, że kluczem jest nie tylko technologia, ale też procedury.

Zdecydowanie. Technologia jest narzędziem – ale musi być częścią większej całości: przemyślanego systemu, który łączy ludzi, sprzęt, oprogramowanie i procedury. Tylko wtedy możemy mówić o realnym bezpieczeństwie. I tylko wtedy technologie mogą spełniać swoją rolę. Nie tylko jako środek reakcji, ale jako aktywny element prewencji. •



C&C Partners Sp. z o.o.
ul. 17 Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl



Sztuczna inteligencja w wielkim mieście



Wiele miast na całym świecie wykorzystuje sztuczną inteligencję oraz techniki uczenia maszynowego w celu zbierania danych, usprawniania nadzoru oraz utrzymywania bezpieczeństwa publicznego. Szlachetnemu celowi, jakim jest bezpieczeństwo, muszą towarzyszyć odpowiednie przepisy. Inaczej obudzimy się w świecie z „Raportu mniejszości”.

Jan T. Grusznic



Zacznijmy od tego, że przywykliśmy do widoku kamer monitoringu wizyjnego w przestrzeni publicznej. Stały się już powszechnym narzędziem zapobiegania przestępczości i wykroczeniom w miejscach publicznych i prywatnych. Większość z nich pomaga w rozwiązywaniu spraw związanych z przestępstwami po ich popełnieniu lub w identyfikacji sprawców.

Daj palec, wezmą rękę. Tak trochę jest z kamerami. Przywykliśmy do tego, że są pomocne, teraz chcemy, by potrafiły jeszcze więcej. W związku z tym rośnie zapotrzebowanie na bardziej zaawansowane i inteligentne środki monitorowania naruszeń, zapobiegania przestępstwom i udzielania pomocy ofiarom. Stąd coraz większa popularność uczenia maszynowego (ML) oraz sztucznej inteligencji, które rewolucjonizują funkcje kamer, powodując poszerzenie zakresu zastosowań kamer, które wykracza poza tradycyjny dozór. Dzięki algorytmom uczenia maszynowego i sztucznej inteligencji możliwa jest m.in. analiza danych w czasie rzeczywistym, co redefiniuje podejście do bezpieczeństwa. Nim jednak przejdziemy do tego, jakie konsekwencje ma stała obecność inteligentnego monitoringu w miastach, przyjrzyjmy się dokładnie, co tak naprawdę potrafi.

Kamery inteligentne, czyli jakie?

Najczęściej, gdy mowa jest o tzw. inteligentnych kamerach, pierwsze skojarzenie dotyczy klasyfikacji obiektów, ewentualnie wykrywania nietypowych zachowań, jak nagle gromadzenie się tłumu, czyjaś paniczna ucieczka bądź pojawienie się intruza w strefie zazwyczaj niedostępnej dla osób postronnych. Tymczasem inteligentne kamery potrafią o wiele więcej. Algorytmy SI analizują zmiany jakości obrazu i powiadamiają o znacznym jego zubożeniu. Analizują obraz pod kątem tła oraz przestrzeni o dużej częstotliwości zmian, aby odpowiednio dobrać parametry kompresji, naświetlenia lub wzmocnienia, zapewniając optymalny poziom jakościowy danych wejściowych. Algorytmy SI w kamerach nieprzerwanie analizują strumień danych, aby docelowo zbudować model obserwowanej sceny. Dzięki temu zapewniają lepszy poziom detekcji obiektów, ponieważ automatycznie ogranicza analizowany obszar, nakładając na niego siatkę 3D. I chociaż takie informacje nie są w żaden sposób „rysowane” na obrazie, to są dostępne w postaci strumienia metadanych wysyłanych równoległe do strumienia wideo. Metadane są złożonym opisem zawartości obrazu wykorzystywanym na potrzeby dalszej

analizy. Coraz częściej mają format zestandaryzowany zaproponowany przez organizację ONVIF w profilu M, przez co stały się rozwiązaniem agnostycznym sprzętowo. Zaznaczam tutaj, że liczba przesyłanych danych zależy od samego modelu kamery. Nie można też zapomnieć, że dzięki funkcjom predykcyjnym algorytmy zawczasu informują o możliwej awarii urządzenia.

Moc obliczeniowa kamer dozoru wizyjnego nieprzerwanie rośnie, jednak mają one swoje ograniczenia. Przykładem są kamery do odczytu tablic rejestracyjnych. W wielu przypadkach potrafią podać informację o marce, modelu i kolorze pojazdu – problem pojawia się, gdy trzeba zidentyfikować pojazd bez tablic rejestracyjnych. W przeważających systemach algorytmy najpierw próbują odczytać tablicę rejestracyjną. Dopiero potem przystępują do zbierania dalszych danych o pojeździe. Efekt? Nie ma tablicy – nie ma pojazdu. Innym przykładem jest rozpoznanie twarzy (*Facial Recognition* – FR). Współczesne kamery całkiem dobrze radzą sobie z wykrywaniem twarzy na obrazie. Jednak nie dysponują wystarczającą mocą obliczeniową, aby prawidłowo i w krótkim czasie mogły ją rozpoznać. Czym innym bowiem „zrozumienie”, że fragment obrazu to twarz człowieka, a czym innym jej rozpoznanie i przypisanie do konkretnej osoby.

Gdy doba jest za krótka, przydaje się metaanaliza

Systemy dozoru wizyjnego są znacząco pomocne podczas prowadzenia różnego rodzaju dochodzeń. Zapis obrazu z kamer jest o tyle istotny, że pokazuje zdarzenie takim, jakie rzeczywiście było. Pamięć naocznych świadków, o ile są, bywa bardzo często zawodna. Pod tym względem zapis wideo jest bezkonkurencyjny. Ale... im więcej nagrań, tym więcej danych do analizy. Wyzwaniem dla operatorów monitoringu miejskich jest zatem analiza coraz większych zbiorów danych. Czas potrzebny na odnalezienie właściwego nagrania staje się coraz dłuższy. W odróżnieniu od doby, która – jak świat światem – trwa 24 godziny. W tym przypadku pomocne okazują się rozwiązania wykorzystujące połączenie analizy wideo (po stronie kamer i serwera) z algorytmami głębokiego uczenia do wykrywania, klasyfikowania i wyszukiwania. Wspomniane wcześniej metadane zasadniczo przypisują cyfrowe znaczenie każdej klatce wideo, skupiając się na obiektach w niej zawartych. Innymi słowy, dodają opis sceny. Metadane mogą obejmować lokalizację, czas, kolory, rozmiary, kształty, współrzędne, trasę, prędkość, czas trwania sceny, kierunek przemieszczania, typ, klasę i podklasę obiektu itd. Dzięki filtrom wyszukiwania operator może szybko przejrzeć wideo, aby znaleźć interesujące osoby, przedmioty i pojazdy. Możliwość przejrzania godzin nagrań w ciągu kilku sekund jest bezcenna.

Metadane są ułatwieniem także dla instytucji zarządzających miastem, choćby do badania wzorców zachowań w czasie. Kompleksowe oprogramowanie do analizy wizyjnej gromadzi i agreguje dane, takie jak natężenie i wzorce ruchu, statystyki zajętości i czas przebywania – prezentując je na łatwych w użyciu pulpitych nawigacyjnych z wykresami i tzw. mapami ciepła (*heat maps*), będących graficznym przedstawieniem danych, w którym wartości są reprezentowane kolorami, zwykle na tle obrazu lub planu przestrzeni (np. sklepu, hali, parkingu, lotniska). *Heat mapa* pokazuje miejsca, gdzie ruch ludzi był największy (najczęściej uczęszczane obszary), zaznaczając te miejsca ciepłymi kolorami

(np. czerwony, pomarańczowy). Miejsca mniej uczęszczane są przedstawiane jako zimniejsze kolory (np. niebieski, zielony). Choć *heat mapa* może też dotyczyć innego rodzaju aktywności.

Dzięki tym statystykom możliwe jest opracowanie trendów służących potem do skonfigurowania alarmów dla sytuacji odbiegających od tych trendów, anormalnych.

Słowa mają moc

Na atrakcyjności zyskuje nowy sposób wyszukiwania materiału wizyjnego – wyszukiwanie tekstowe. Brzmi dziwnie, ale jest sensowne. Wyszukiwanie tekstowe również korzysta z metadanych generowanych przez kamery. Obejmują one typ obiektu (osoba, typ pojazdu, obiekt nieznany, itp.) oraz jego atrybuty, takie jak kolor, prędkość, lokalizacja i sygnatura czasowa. Tradycyjnie wyszukiwanie przy użyciu metadanych wykonywane jest za pomocą predefiniowanych filtrów wyszukiwania, zawierających stałe opisy obiektów z listy, np. typ obiektu (np. „pojazd”), typ pojazdu (jeśli dotyczy, np. „samochód”), kolor (np. „niebieski”) i inne. Metoda wyszukiwania tekstowego pozwala natomiast na tworzenie własnych filtrów wyszukiwania. Jeśli bowiem wyszukiwanie ograniczone jest tylko do wstępnie sklasyfikowanych danych, to wprowadzić da precyzyjne wyniki, ale nie umożliwi wykrycia tych obiektów, które wcześniej nie zostały zdefiniowane. Wyszukiwanie tekstowe zapewnia swobodę i elastyczność wyszukiwania przy użyciu własnych słów. Można opisać dowolny obiekt bardziej szczegółowo, używając języka naturalnego i skojarzeń, aby doprecyzować wyszukiwanie i uzyskać więcej wyników. Przykładem zapytania jest choćby „osoba w czerwonej kurtce i z plecakiem”. Przeszukiwanie wideo za pomocą pytań w języku naturalnym oznacza możliwość zastosowania niemal nieograniczonych kryteriów wyszukiwania. Za rozwiązaniem stoi model podstawowy tekst-obraz, który został wytrenowany na dużych zbiorach danych zawierających taką parę informacji, czyli tekst plus obraz. Jest to model typu zero-shot, który dopasowuje tekst do odpowiednich obrazów. Model typu zero-shot (zero-shot model) to taki model uczenia maszynowego, który potrafi rozwiązywać zadanie, którego nigdy wcześniej nie widział w danych treningowych, bez dodatkowego uczenia. Na przykład, mając zestaw obrazów zwierząt do sklasyfikowania, wraz z pomocniczymi opisami tekstowymi tego, jak wyglądają zwierzęta, model sztucznej inteligencji, który został wyszkolony do rozpoznawania koni, ale nigdy nie otrzymał zebry, potrafi znaleźć zebra na obrazie, gdyż wie, że zebra wygląda jak niewielki koń w białe czarne pasy. Ta umiejętność ma zasadnicze znaczenie dla zapewnienia optymalnej wydajności w dopasowywaniu języka naturalnego do obrazów.

Zawsze jest jakieś „ale”

Miasta wykorzystują SI, aby zapewnić swoim obywatelom bezpieczeństwo. Co nie znaczy, że mogą nie przejmować się ich prywatnością. Nadzór i predyktoryjne działania za pomocą sztucznej inteligencji to najbardziej kontrowersyjny trend w systemach dozoru wizyjnego, który ma ważne implikacje dla przyszłości miast i społeczeństw. Istnieją pewne wątpliwości, czy wpływ sztucznej inteligencji na funkcjonowanie miast to wyłącznie „cud, miód i orzeszki”. Najbardziej podstawowym problemem jest prywatność, ale często toczą się debaty na temat sztucznej inteligencji z innych perspektyw, takich jak jej wpływ na miejsca

pracy, gospodarkę i przyszłość pracy. Nie można zatem oddzielić dyskusji na temat inwigilacji i predyktoryjnych działań od niedawnych debat na temat wymiaru społecznego i etycznego wprowadzenia sztucznej inteligencji do nadzoru nad miejską przestrzenią. Sam dozór wizyjny w domenie publicznej został już społecznie zaakceptowany, ale miasta badają możliwości przewidywania przestępczości poprzez analizę danych z systemów dozoru wizyjnego w celu poprawy bezpieczeństwa. Dzięki wykorzystaniu SI analiza obrazów zapewnia szybsze podejmowanie działań. Uczenie maszynowe i analiza dużych zbiorów danych umożliwiają poruszanie się po ogromnych ilościach danych w celu identyfikacji wzorców, korelacji i trendów. Kiedy istnieją właściwe relacje, technologia jest warstwą, która wspiera organy ścigania w lepszym wykonywaniu ich pracy. Ostatecznym celem jest stworzenie elastycznych systemów bezpieczeństwa, które będą w stanie wykrywać sieci przestępcze lub terrorystyczne oraz podejrzaną aktywność, a nawet przyczyniać się do skuteczności systemów wymiaru sprawiedliwości. Kluczowym pytaniem pozostaje, w jaki sposób osiągnąć te cele przy jednoczesnym poszanowaniu prywatności i praw obywatelskich.

Eksperti twierdzą, że prawie niemożliwe jest zaprojektowanie powszechnie stosowanych etycznych systemów sztucznej



inteligencji ze względu na ogromną złożoność różnorodnych kontekstów, które muszą one obejmować. Wszelkim postępom w dziedzinie sztucznej inteligencji w zakresie nadzoru i predykcyjnego dozoru muszą towarzyszyć dyskusje na temat kwestii etycznych i regulacyjnych. Mimo że propozycja wartości tych technologii może wydawać się atrakcyjna z perspektywy przypadków użycia, wolności i prawa obywatelskie muszą być chronione przez odpowiednie przepisy dotyczące prywatności i praw człowieka. Chociaż jest to kontrowersyjna kwestia w krajach zachodnich, w krajach azjatyckich, a szczególnie w Chinach, podobnych wątpliwości jest zdecydowanie mniej. Badanie przeprowadzone przez Deloitte wykazało znaczne różnice w akceptacji i atrakcyjności tych technologii między regionami. Zarówno inwigilacja, jak i predykcyjne działania policyjne są uważane za niepożądane w regionach geograficznych bardziej dbających o prywatność, takich jak UE i Ameryka Północna. Obywatele krajów Ameryki Łacińskiej i Azji wykazują się w tej kwestii większą wyrozumiałością.

Sztuczna inteligencja ma swoje prawa

Unia Europejska przygotowała ustawę o sztucznej inteligencji, która jest znana jako AI Act. Ma ona zapewnić rozwój i wykorzystywanie sztucznej inteligencji w sposób bezpieczny, niezawodny

i przejrzysty. Unijna ustawa ma chronić przed wszelkimi negatywnymi konsekwencjami sztucznej inteligencji. Dlatego też w pewien sposób wymusza na organizacjach korzystających z takich systemów zapewnienie, że ich SI nie dyskryminuje ludzi, nie wprowadza ich w błąd oraz że ich aplikacje nie są wykorzystywane w sposób nieetyczny lub nawet niezgodny z prawem. Użytkownicy powinni być świadomi, że wchodzi w interakcję ze sztuczną inteligencją, bez względu na rodzaj systemu – czy jest to aplikacja generująca obrazy, są to treści audio lub wideo, manipulacje za pomocą *deep fake*, czy systemy dozoru wizyjnego.

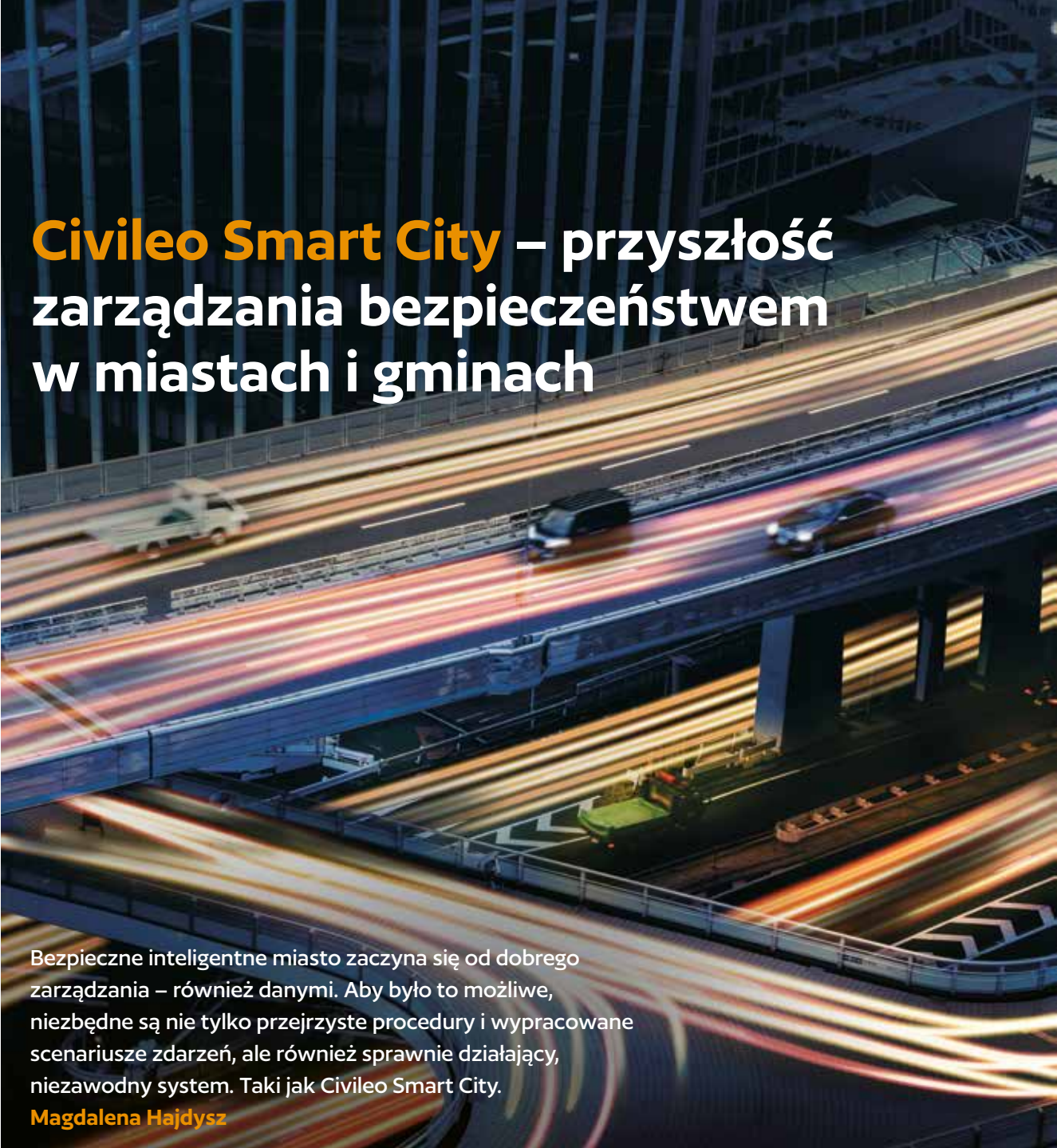
AI Act wprowadza przepisy, które mają na celu ochronę prywatności użytkowników i danych, na których opierają się systemy AI. Szczególną uwagę poświęca się zapewnieniu, że dane osobowe są zbierane, przetwarzane i przechowywane zgodnie z ogólnymi zasadami ochrony danych osobowych, takimi jak Rozporządzenie o Ochronie Danych Osobowych (RODO). Dotyczy to m.in. zabezpieczenia danych wykorzystywanych przez systemy AI, minimalizacji ryzyka nieuprawnionego dostępu do nich oraz zapewnienia przejrzystości w zakresie ich wykorzystania. W tym przypadku warto wrócić do systemów FR, tj. systemów AI, które stosują biometrię, takie jak rozpoznawanie twarzy i są objęte szczególnymi regulacjami. AI Act wprowadza rygorystyczne zasady stosowania takich technologii, szczególnie w kontekście ochrony prywatności obywateli. W niektórych przypadkach (np. w przestrzeni publicznej) wprowadza całkowity zakaz stosowania rozpoznawania twarzy, chyba że istnieją wyraźne uzasadnienia (np. w walce z terroryzmem).

Co do zasady zgodnie z przepisami unijnego AI Act określone praktyki wykorzystujące systemy sztucznej inteligencji zostały uznane za sprzeczne z unijnymi wartościami i zasadami ochrony podstawowych praw oraz wolności. Zdecydowanie zakazane jest stosowanie systemów AI do oceny ryzyka popełnienia przestępstwa przez osoby fizyczne wyłącznie na podstawie ich profilu lub cech osobowościowych („Raport mniejszości” pozostać ma więc w dalszym ciągu filmową fikcją). Profilowanie tego typu może prowadzić do nieproporcjonalnych i nieuzasadnionych decyzji, które mogą stygmatyzować jednostki na podstawie ich osobistych cech lub przewidywań, a nie na podstawie rzeczywistych, weryfikowalnych faktów związanych z ich działalnością przestępczą. Zakazane jest również tworzenie lub rozbudowywanie baz danych do rozpoznawania twarzy, zwłaszcza gdy wizerunki są pozyskiwane w sposób niekontrolowany (np. poprzez hurtowe pobieranie danych z Internetu, tzw. scrapowanie czy nagrania systemów dozoru wizyjnego). Zakazane jest również stosowanie systemów AI do zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej, z wyjątkiem sytuacji, gdy jest to absolutnie konieczne do celów takich jak:

- poszukiwanie ofiar uprowadzeń, handlu ludźmi lub wykorzystywania seksualnego,
- zapobieganie poważnemu zagrożeniu życia lub bezpieczeństwa fizycznego,
- lokowanie lub identyfikowanie osób podejrzanych o popełnienie przestępstw.

Tego typu identyfikacja musi odbywać się zgodnie z przepisami prawa krajowego, a jej wykorzystanie wymaga uprzedniego zezwolenia przez organ wymiaru sprawiedliwości lub inny niezależny organ administracyjny. Przepisy prawa mają jednak to do siebie, że zawsze znajdzie się ktoś, kto zechce je obejść. •





Civileo Smart City – przyszłość zarządzania bezpieczeństwem w miastach i gminach

Bezpieczne inteligentne miasto zaczyna się od dobrego zarządzania – również danymi. Aby było to możliwe, niezbędne są nie tylko przejrzyste procedury i wypracowane scenariusze zdarzeń, ale również sprawnie działający, niezawodny system. Taki jak Civileo Smart City.

Magdalena Hajdysz

Civileo Smart City to polski system do zarządzania bezpieczeństwem publicznym i infrastrukturą miejską – wyjątkowy na tle konkurencyjnych rozwiązań, dzięki unikatowej architekturze otwartej integracji i zaawansowanej analityce.

W pełni integrujący system VMS nowej generacji

Możliwości tradycyjnych systemów monitoringu kończą się tam, gdzie zaczynają się ograniczenia integracyjne. Civileo Smart City w swojej najnowszej wersji 2.0 wychodzi poza te ramy. Jako jeden z nielicznych systemów VMS (Video Management System) umożliwia pełną integrację z urządzeniami i systemami już działającymi u zamawiającego, niezależnie od ich producenta czy

protokołu komunikacyjnego. To oznacza możliwość rozbudowy istniejącej infrastruktury bez konieczności kosztownej wymiany całego środowiska.

System obsługuje nie tylko kamery, rejestratory i ściany wizyjne, ale też stacje pogodowe, czujniki środowiskowe, moduły audio, systemy zarządzania ruchem (ITS), tablice zmiennej treści, a także urządzenia i programy do inteligentnego zarządzania parkingami. Civileo Smart City wspiera także instytucje odpowiedzialne za bezpieczeństwo miast, ułatwiając stałe monitorowanie warunków środowiskowych, w tym poziomu wód, jakości powietrza oraz natężenia hałasu. Dzięki zaawansowanym algorytmom detekcji pozwala na reagowanie w czasie rzeczywistym oraz działania prewencyjne.

Dzięki modułowej budowie Civileo może być łatwo skalowany od pojedynczego osiedla po całe miasta i regiony.

Sztuczna inteligencja i edge computing

Wprowadzenie Civileo pozwala na aktywne zarządzanie zdarzeniami. Zaawansowane analityki obrazu i dźwięku umożliwiają bowiem automatyczne wykrywanie nietypowych sytuacji, takich jak kolizja, wtargnięcie na jezdnię, bójka, pożar, niszczenie mienia przez wandalę, porzucenie przedmiotu, krzyk czy dźwięk tłuczonego szkła. Co istotne, analiza może być prowadzona nie tylko przez oprogramowanie zainstalowane na serwerze, ale również przez urządzenia pracujące na brzegu sieci (edge AI), czyli kamery

Ilustracje: Freepik

i rejestratory. To znacząco zwiększa wydajność i elastyczność systemu i pozwala reagować odpowiednim służbom, zanim jeszcze informacja trafi do centrum.

Civileo Smart City może również zrealizować dowolne przygotowane wcześniej scenariusze zautomatyzowanych działań, np. uruchomić syrenę alarmową, wyświetlić ostrzeżenie na tablicy LED, wysłać komunikat głosowy, a także powiadomić mieszkańców zagrożonego obszaru za pomocą aplikacji Vileo. To poziom działania, który do niedawna był wyłącznie domeną systemów militarnych lub przemysłowych.

Komunikacja z mieszkańcami w czasie rzeczywistym

Civileo dba także o transparentną relację z mieszkańcami. Zintegrowana z systemem aplikacja Vileo umożliwia operatorom monitoringu miejskiego i centrom zarządzania kryzysowego wysyłanie powiadomień typu *push*, umieszczanie komunikatów na publicznych kontach w mediach społecznościowych bądź wysyłanie wiadomości skierowanych bezpośrednio do wybranych grup osób, np. mieszkających w danych miejscach. Może to być informacja o pożarze, awarii, utrudnieniach drogowych lub zalecenie ewakuacji. Aplikacja jest również wyposażona w zaawansowany czat AI, zasilany szczegółowymi informacjami dotyczącymi

danej dzielnicy, w której mieszka użytkownik, w tym związanymi z bezpieczeństwem. To funkcja unikatowa na rynku europejskim – gdzie większość systemów VMS skupia się wyłącznie na nadzorze, bez aspektu aktywnej, selektywnej i bezpiecznej komunikacji.

Innowacyjność i bezpieczeństwo potwierdzone w praktyce

Civileo Smart City to rozwiązanie w całości opracowane w Polsce i zgodne z wymogami RODO, Ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz wytycznymi KPRM, a także gotowe na wytyczne dyrektywy NIS2.

System jest kompatybilny z klasycznymi rejestratorami, ale także gotowy do współpracy z infrastrukturą IoT, 5G oraz platformami typu *open data*. Wyróżnia się unikatowym, otwartym interfejsem API oraz neutralnością sprzętową, co czyni go idealnym dla jednostek samorządu terytorialnego, które chcą budować Smart City etapami, bez uzależniania się od jednego producenta.

Na tle konkurencji Civileo wyróżnia także możliwość tworzenia tzw. scenariuszy zdarzeń – zdefiniowanych ciągów reakcji systemu na konkretne sytuacje oraz generowanie przejrzystej dokumentacji, raportów oraz wszelkich podjętych przez służby działań, a także

zautomatyzowanego archiwum z możliwością szybkiego wyszukiwania po dowolnych danych i łatwego nagrywania materiału na wybrany nośnik zewnętrzny.

Civileo – system, który się uczy

Dzięki zastosowaniu głębokiego uczenia maszynowego oraz innowacyjnego podejścia do treningu modeli AI i zarządzania nimi – co z kolei wspiera kompatybilny system SPIN AI – Civileo adaptuje się do warunków konkretnego miasta. Rozpoznaje typowe wzorce ruchu, analizuje zachowania mieszkańców, rozróżnia fałszywe alarmy i na ich podstawie dostosowuje czułość analityk. System „uczy się” zatem lokalnego kontekstu, uwzględniając nawet takie zmiany, jak pogoda czy pory roku. Dzięki temu zmniejsza się liczba fałszywych alarmów, a rośnie efektywność operacyjna.

Civileo Smart City to coś więcej niż system monitoringu – to otwarta, inteligentna platforma bezpieczeństwa miejskiego przyszłości, tworzona z myślą o samorządach, które chcą efektywnie zarządzać ryzykiem, infrastrukturą i komunikacją z mieszkańcami. •



OKE Poland
ul. Jana z Kolna 11
80-864 Gdańsk
www.oke.pl



Smart city bezpieczne dzięki narzędziom Hikvision

Rozwój współczesnych miast to nie tylko ich intensywna rozbudowa. To przede wszystkim inne podejście do funkcji miasta. Ludzie oczekują bowiem, że będą to miejsca wygodne, ale i bezpieczne. Takie właśnie są smart city. Aby miasto było smart, trzeba jego tkankę wyposażać w różne narzędzia.

Michał Swoboda

Inteligentne miasto potrzebuje inteligentnych systemów, m.in. monitoringu wizyjnego, który służb miejskich nie zastąpi, ale zoptymalizuje i ułatwi ich pracę. Firma Hikvision, będąc globalnym liderem w branży CCTV i technologii AIoT, oferuje kompleksowe rozwiązania – od kamer z analizą brzegową po rozbudowane systemy zarządzania i analizy serwerowych – dopasowane do potrzeb różnych miast.

Wielopoziomowa architektura analizy obrazu

Nowoczesne miasta korzystają dziś z trójpłaszczyznowej struktury analitycznej. Pierwszy poziom stanowi analiza na brzegu sieci (*edge analytics*). owoczesne kamery IP Hikvision z serii DeepinView i DarkFighter 2.0 potrafią samodzielnie analizować obraz pod kątem typów obiektów, cech obiektów oraz

zachowania. Dzięki temu kamery mogą dużo skuteczniej wykrywać zagrożenia oraz dostarczać wielu istotnych informacji, takich jak liczba osób lub pojazdów, cechy szczególne obiektów (np.: marka pojazdu czy posiadanie kasku), numery tablic rejestracyjnych czy też natężenie ruchu drogowego. Przetwarzanie danych bezpośrednio przez kamerę odciąża infrastrukturę i umożliwia szybszą reakcję obsługi.

Drugi poziom to analiza dokonywana przez wyspecjalizowane jednostki obliczeniowe, jakimi są rejestratory DeepinMind nowej generacji Hikvision NVR 5.0, wyposażone w układy AI i takie funkcje, jak AcuSearch. To one pozwalają na szybkie i precyzyjne wyszukiwanie zdarzeń poprzez szybką analizę metadanych. Technologia głębokiego uczenia zawarta w tych rejestratorach może uzupełnić system o dodatkowe funkcje (np.

identyfikacja twarzy) lub zapewnić zaawansowane algorytmy detekcji starszym kamerom, które nie mają istotnych funkcji.

Trzecim poziomem są analizy serwerowe (VMS i niezależne silniki AI). W tym przypadku platforma HikCentral Professional v3.0 służy do centralnego zarządzania i analizy danych pochodzących nawet z tysięcy kanałów wideo. Wprowadzenie klastrów sprzyja obsłudze systemów metropolitalnych, zapewniając nie tylko rejestrację wielu danych, lecz także analizę wideo, integrację z systemami alarmowymi, kontroli dostępu oraz mapami GIS.

Smart City to Safe City

Rozwiązania Safe City proponowane przez Hikvision stanowią odpowiedź na wyzwania nowoczesnych aglomeracji. Kamery multisensorowe, PTZ oraz panoramiczne





rejestrują obraz w wysokiej rozdzielczości. Nawet w niesprzyjających warunkach oświetleniowych. Dzięki integracji z analityką wyposażoną w moduły sztucznej inteligencji osoby odpowiedzialne za zarządzanie różnymi aspektami funkcjonowania miasta mogą szybko identyfikować zagrożenia, monitorować transport publiczny, wykrywać incydenty drogowe i analizować natężenie ruchu.

Rozwiązania Hikvision po prostu znacząco poprawiają efektywność operatorów monitoringu miejskiego. Automatyczne powiadomienia, dynamiczne mapy zdarzeń, możliwość śledzenia obiektów przez kamery PTZ oraz klasyfikacja alarmów za pomocą AI skracają czas reakcji i pozwalają operatorowi skupić się na najważniejszych sytuacjach. A funkcje raportowania i inteligentnego wyszukiwania zdarzeń (m.in. według typu obiektu, koloru odzieży czy

kierunku poruszania się), którymi dysponują HikCentral Pro i NVR 5.0, realnie wpływają na jakość i szybkość pracy zespołów zarządzających bezpieczeństwem.

Zarządzanie danymi i skalowalność

Im więcej urządzeń podłączonych do sieci pracuje w przestrzeni miejskiej, tym więcej danych jest zbieranych i tym trudniejsze jest zapanowanie nad nimi. Zarówno nad ich ilością, jak i nad skutecznym ich zarządzaniem. Dlatego Hikvision proponuje systemy skalowane, od lokalnych rozwiązań w ramach jednej dzielnicy, po pełne systemy miejskie z integracją danych z różnych źródeł (kamery monitoringu, czujniki IoT, pojazdy służb miejskich). Taki model pozwala na dostosowanie systemu do rozwoju miasta, a jednocześnie daje czas niezbędny na

przygotowanie się do zarządzania danymi. Otwarte API umożliwia integrację z działającymi już platformami zarządzania kryzysowego i systemami ITS.

W Hikvision chcemy, aby miasta były bezpieczne, inteligentne i zrównoważone. Dlatego wspieramy rozwój miejskiej infrastruktury, oferując nie tylko nowoczesne kamery, ale także wielopoziomową analizę danych, integrację z systemami miejskimi i wsparcie dla operatorów. Dzięki platformie **HikCentral Professional v3.0**, nowej generacji **NVR 5.0** oraz kamerom z analizą brzegową, możliwe jest tworzenie skalowalnych i elastycznych ekosystemów bezpieczeństwa miejskiego. •



Hikvision Poland

ul. Zwirki i Wigury 16B,
02-092 Warszawa
<https://www.hikvision.com/pl/>



Bezprecedensowe środki bezpieczeństwa w Watykanie

Podczas tegorocznego konklawe oraz zbliżających się uroczystości rozpoczynających nowy pontyfikat Watykan we współpracy z włoskimi służbami wdrożył najbardziej zaawansowany system bezpieczeństwa w historii papieskich ceremonii. Złożony z tradycyjnych oraz nowoczesnych elementów plan zabezpieczeń stworzył prawdziwą „fortecę” wokół Watykanu.

Monika Żuber-Mamak





Trzy pierścienie ochrony

Bezpieczeństwa placu Świętego Piotra i okolic strzegło ponad 2000 funkcjonariuszy różnych służb, tworząc trójwarstwowy system ochrony. Wprowadzono patrole piesze, konne oraz dodatkowe jednostki policji wodnej na Tybrze, zapewniając kompleksową kontrolę terenu. Policja, karabinierzy, strażacy i służby miejskie wspólnie monitorowały sytuację w Watykanie i przyległych dzielnicach Rzymu. Łącznie ponad 4 tys. funkcjonariuszy zostało rozmieszczonych w strategicznych punktach miasta. Czasowe zakazy ruchu kołowego w bezpośrednim sąsiedztwie Watykanu znacząco zwiększyły bezpieczeństwo pieszych uczestników uroczystości. A było ich sporo, podczas oczekiwania na biały dym, na placu Świętego Piotra zgromadziło się 150 tys. osób. Na czas konklawe w celu ochrony przestrzeni powietrznej wprowadzono strefę zakazu lotów nad Watykanem, a także zastosowano technologie przeciwdziałające dronom, w tym tzw. bazooki antydronowe.

Podczas poprzedniej inauguracji na samym placu zgromadziło się 150-200 tysięcy wiernych oraz delegacje ze 132 państw. Służby włoskie ściśle współpracowały wówczas z przedstawicielami agencji bezpieczeństwa z innych krajów, aby zapewnić ochronę delegacjom zagranicznym. Wykorzystano zaawansowane systemy monitoringu tłumu, pozwalające na szybkie wychwycenie niepokojących zachowań i natychmiastową reakcję. Kontrole bezpieczeństwa przeprowadzano również na głównych węzłach komunikacyjnych: lotnisku Fiumicino, w porcie Civitavecchia oraz na dworcu Termini. Tym razem władze miasta spodziewały się, że podczas inauguracji pontyfikatu Watykan odwiedzi ok. 250 tys. osób. Stąd jeszcze bardziej rygorystyczne środki zaradcze. Aby zapewnić bezpieczeństwo podczas tego historycznego wydarzenia, władze Rzymu i Watykanu wprowadziły podwójne punkty kontrolne w rejonie placu Świętego Piotra oraz wzdłuż Via della Conciliazione, z wykorzystaniem detektorów metalu i skanerów bagażu. Prowadzono inspekcje koszy na śmieci, studzienek kanalizacyjnych i innych potencjalnych miejsc ukrycia niebezpiecznych przedmiotów.

Elektroniczny bunkier w Kaplicy Sykstyńskiej

Już w 2013 roku, podczas konklawe, na którym wybrano papieża Franciszka, urzędnicy watykańscy użyli klatki Faradaya do blokowania sygnałów elektromagnetycznych. Teraz Kaplicę Sykstyńską przekształcono w prawdziwy „elektroniczny bunkier”. Między innymi zainstalowano dodatkową podłogę, pod którą ukryte zostały urządzenia zakłócające sygnały, a także zastosowano specjalne płytki blokujące sygnały, aby zapobiec elektronicznemu podsłuchowi. Okna kaplicy zabezpieczono specjalną folią chroniącą przed obserwacją z powietrza, a cały obszar objęto strefą zakazu lotów, by zapobiec zarówno potencjalnym zagrożeniom, jak i próbom naruszenia tajemnicy obrad przez wykorzystanie dronów czy innych urządzeń latających.

Ekskomunika karą za niedyskrecję

Watykańska służba cyberbezpieczeństwa wdrożyła systemy monitorujące urządzenia końcowe oraz wykorzystujące sztuczną



Żandarmeria Watykańska dysponowała jednostką szybkiego reagowania (GIR) oraz nowoczesnym centrum operacyjnym z dostępem do tysięcy kamer monitoringu rozmieszczonych na terenie Watykanu.

inteligencję do wykrywania potencjalnych zagrożeń. Zespoły ekspertów nieustannie analizowały ruch w sieci, wychwytyując próby ataków hakerskich czy działań dezinformacyjnych. Wszyscy pracownicy pomocniczy, w tym personel techniczny i obsługa, złożyli przysięgę zachowania absolutnej tajemnicy. Zgodnie z wielowiekową tradycją złamanie tej przysięgi grozi ekskomuniką.

Elitarne formacje ochronne

Główną odpowiedzialność za bezpieczeństwo ponosiły dwie formacje: Gwardia Szwajcarska oraz Żandarmeria Watykańska. Choć gwardziści szwajcarscy kojarzeni są głównie z barwnymi, historycznymi strojami, stanowią w rzeczywistości nowoczesną jednostkę wojskową, profesjonalnie przeszkoloną w zakresie ochrony osobistej i przeciwdziałania zamachom.

Żandarmeria Watykańska, odpowiedzialna za bezpieczeństwo wewnętrzne, dysponowała jednostką szybkiego reagowania (GIR) oraz nowoczesnym centrum operacyjnym z dostępem do tysięcy kamer monitoringu rozmieszczonych na terenie Watykanu i w jego okolicach.

Inauguracja pod specjalnym nadzorem

Tegoroczne konklawe pokazało, że nowoczesne rozwiązania znajdują zastosowanie nawet w przypadku wydarzeń o tak wielowiekowej tradycji jak konklawe, którego obrady odbyły się w całkowitej izolacji od świata zewnętrznego. Wdrożone rozwiązania bezpieczeństwa pokazują, że nawet najbardziej tradycyjne instytucje potrafią adaptować się do zmieniających się warunków współczesnego świata. •

Monika Żuber-Mamak
redaktorka „a&s Polska”



Czy bezbiletowe parkingi Freeflow to przyszłość parkowania w miastach?

Bezbiletowe rozwiązanie dla nowoczesnych miast czy model o ograniczonym zastosowaniu?



Freeflow to nowoczesny bezszlabanowy system parkowania. Kierowcy nie zatrzymują się przy wjeździe, nie pobierają biletu, nie czekają w kolejce przy wyjeździe. System automatycznie rozpoznaje numery rejestracyjne pojazdów (*License Plate Recognition, LPR*), rejestruje czas postoj i umożliwia cyfrową płatność przez aplikację, online lub w automacie. Taki parking jest bardziej dostępny, intuicyjny i nowoczesny.

Gdzie Freeflow sprawdza się najlepiej?

System bezszlabanowy już dziś działa z sukcesem na wielu miejskich parkingach, przy centrach handlowych, lotniskach czy biurach.

Sprawdza się szczególnie wtedy, gdy:

- zachodzi duża rotacja pojazdów,
- użytkownicy oczekują szybkości i wygody,
- właściciele chcą zwiększyć przychody i zmniejszyć koszty infrastrukturalne.

Czy Freeflow ma ograniczenia?

Owszem – nie wszędzie można całkowicie zrezygnować z fizycznej kontroli dostępu. Strefy premium, obiekty rządowe czy zamknięte wspólnoty mieszkaniowe często wymagają modeli hybrydowych lub półotwartych. Kluczowe dla sukcesu pozostaje także skuteczne egzekwowanie opłat – bez szlabanów to jedyny element pilnujący uczciwości systemu.

Operatorzy coraz częściej wybierają Freeflow, ponieważ...

...zapewnia lepsze doświadczenie użytkownika. Kierowcy doceniają płynność obsługi – brak konieczności interakcji z urządzeniami, brak biletów papierowych i możliwość zapłaty w dowolnym momencie – to elementy, które przekładają się na wyższy komfort i lojalność klientów.

...mniejszym kosztem towarzyszy większa wydajność. Brak szlabanów, drukarek biletów czy czytników kart oznacza mniej awarii i mniej interwencji serwisowych. Freeflow redukuje nakłady operacyjne i techniczne, jednocześnie umożliwiając obsługę większej liczby użytkowników bez potrzeby zwiększania personelu.

...rozwiązanie jest elastyczne. Freeflow z łatwością integruje się z systemami rezerwacyjnymi, aplikacjami miejskimi czy usługami MaaS (*Mobility as a Service*). To rozwiązanie, które pozwala miastom i prywatnym operatorom budować bardziej zrównoważony i cyfrowy ekosystem mobilności.

Freeflow to nie tylko technologia – to strategiczna decyzja. Dobrze wdrożony system upraszcza obsługę, to z kolei może przyczynić się do zwiększenia przepustowości parkingów, zminimalizowania liczby niepożądanych incydentów i wpływa na postrzeganie obiektu jako nowoczesnego i wygodnego. Co więcej, dane pozyskiwane w modelu Freeflow pomagają w lepszym planowaniu, optymalizacji i personalizacji usług.

Nie każdy parking może działać w modelu Freeflow. Ale sprawdzi się on idealnie w przypadku tych miast i tych operatorów parkingów, którym zależy na automatyzacji obsługi parkingów, co przekłada się na wygodę użytkowników, ale też niższe koszty obsługi. Coraz więcej inwestorów wprowadza ten model zarządzania parkingiem, doceniając wygodę tego rozwiązania.

Zastanawiasz się, czy Freeflow sprawdzi się również w twojej lokalizacji? Skontaktuj się z nami – pomożemy dobrać optymalne rozwiązanie. •



Procedura korzystania z parkingu Freeflow – od rejestracji po płynny wyjazd dzięki rozpoznawaniu tablic rejestracyjnych i płatnościom mobilnym.



DESIGNA AXESS POLSKA

plac Konesera 12, 03-736 Warszawa
<https://designa.com>
Konrad.Jaworski@designa.com



Polskie profesjonalne
zintegrowane rozwiązania
VMS

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



www.alnetsystems.com



Za kulisami bezpiecznej imprezy

Organizacja imprez masowych to ogromne wyzwanie logistyczne i odpowiedzialność, której najważniejszym aspektem jest zapewnienie bezpieczeństwa uczestnikom. Kluczowe znaczenie mają tu również odpowiednie podstawy prawne oraz współpraca z wyspecjalizowanymi podmiotami branżowymi.

Paweł Korzybski



Bezpieczeństwo imprez masowych w Polsce reguluje przede wszystkim Ustawa z 20 marca 2009 r. o bezpieczeństwie imprez masowych. Określa ona obowiązki organizatorów, wymagania dotyczące ochrony i porządku publicznego, a także procedury uzyskiwania zezwoleń. Dodatkowo należy uwzględnić przepisy ustawy Prawo budowlane, ustawy o ochronie przeciwpożarowej, a także akty wykonawcze dotyczące warunków technicznych obiektów. Organizator imprezy masowej musi m.in. uzyskać zgodę właściwego organu (najczęściej prezydenta, burmistrza miasta), przedłożyć plan zabezpieczenia imprezy, uzgodniony z policją, strażą pożarną, pogotowiem ratunkowym oraz – jeśli dotyczy – innymi służbami. Istotnym elementem tego procesu są również konsultacje z ekspertami.

Skuteczna rekrutacja pracowników ochrony

Wnikliwa i precyzyjna rekrutacja jest niezbędna, ponieważ praca podczas imprez masowych wymaga od pracowników odpowiednich kwalifikacji zawodowych, ale także szczególnych predyspozycji psychofizycznych. Jak podkreśla **Anna Jonik-Borys**,

ekspert PZPO, kandydaci muszą wykazywać się odpornością na stres, umiejętnością pracy pod presją czasu, zdolnością do działania w sytuacjach kryzysowych i wysokim poziomem kultury osobistej. Przykładem właściwego podejścia do rekrutacji jest praktyka profesjonalnych firm ochrony, które już na etapie rozmowy kwalifikacyjnej weryfikują nie tylko kompetencje, ale również motywację, predyspozycje psychologiczne/fizyczne kandydatów. Skutecznym rozwiązaniem w procesie rekrutacji jest zastosowanie testów wiedzy zawodowej. Już na wczesnym etapie procesu doboru pracowników sprawdzamy u kandydatów znajomość procedur ewakuacyjnych, zasad udzielania pierwszej pomocy, technik interwencji czy obsługi nowoczesnych systemów CCTV, KD.

Nowoczesne technologie w służbie bezpieczeństwa

Coraz częściej przy zabezpieczaniu imprez masowych stosuje się nowoczesne technologie, tj. mobilne wieże monitoringu wyposażone w kamery obrotowe, noktowizory, a nawet analizę obrazu. Wieże te mogą być lokowane w newralgicznych punktach terenu imprezy, umożliwiając bieżący monitoring

sytuacji. Z kolei dźwiękowe systemy ostrzegawcze (DSO) pozwalają na szybkie przekazywanie informacji uczestnikom.

Zabezpieczenie medyczne i przeciwpożarowe

Każda impreza masowa musi mieć odpowiednie zabezpieczenie medyczne, które obejmuje m.in. obecność ratowników medycznych, punktów pierwszej pomocy oraz ambulansów. Równolegle należy zapewnić zabezpieczenie ppoż.

Bezpieczeństwo imprez masowych to wielowymiarowy proces, wymagający ścisłej współpracy organizatora z ekspertami, służbami i firmami ochrony. Ustalenia prawne, skuteczna rekrutacja, zastosowanie zaawansowanych technologii oraz przygotowanie na sytuacje kryzysowe – to wszystko składa się na sprawne i bezpieczne przeprowadzenie wydarzenia. •



**Polski Związek
Pracodawców Ochrona**

ul. Koszykowa 61, 00-667 Warszawa
<http://www.pzpochrona.pl>
biuro@pzpochrona.pl



Kamery nasobne w ofercie ASBIS: innowacyjne rozwiązanie dla służb i ratowników



Rozmawiamy z **Tomaszem Mąkowskim**, Product Line Sales Managerem w ASBIS Poland, o tym, jak to się stało, że firma specjalizująca się do tej pory w dystrybucji sprzętu IT zainteresowała się kamerami nasobnymi marki Hytera.



Co spowodowało, że w ofercie ASBIS pojawiły się kamery nasobne marki Hytera. Dlaczego zdecydowaliście się na wprowadzenie na rynek właśnie tego produktu i tej firmy?

ASBIS od wielu lat jest największym w regionie partnerem takich producentów, jak Intel, AMD czy Seagate. Kojarzmy się przede wszystkim z urządzeniami i oprogramowaniem IT, ale działamy też w innych sektorach rynku. To właśnie my uczestniczyliśmy w pierwszym wdrożeniu systemu elektronicznego potwierdzania doręczeń dla sądownictwa jako dostawca specjalistycznych tabletów.

Przed rokiem zdecydowaliśmy, że chcemy poszerzyć nasze portfolio o rozwiązania dla firm i instytucji z sektora infrastruktury krytycznej. Hytera to uznany w wielu krajach dostawca sprzętu i oprogramowania do komunikacji radiowej, który sprawdził się w polskich służbach publicznych. Stąd nasz wybór.

Jakie są najważniejsze cechy kamer nasobnych oferowanych przez ASBIS? Czym wyróżniają się na tle konkurencji?

Przede wszystkim kamery nasobne Hytera są projektowane jako element profesjonalnych systemów bezpieczeństwa i w taki sposób, by wytrzymały nawet najtrudniejsze warunki atmosferyczne. Bateria zapewnia aż 10 godzin pracy, a dodatkowe opcje

ładowarek połączone z systemem Digital Evidence Management (DEM) pozwalają na automatyczne zabezpieczenie zarejestrowanych zdarzeń.

Wybrane modele utrzymują stałą łączność poprzez sieć LTE i umożliwiają dwustronną komunikację operatora z centralą oraz przesyłanie na żywo obrazu i dźwięku do systemu dyspozytorskiego. Nagrania są chronione przed nieautoryzowanym dostępem oraz ewentualną manipulacją.

Dla kogo przeznaczone są kamery nasobne marki Hytera, gdzie są najbardziej przydatne?

Polecamy je przede wszystkim tym osobom, które z różnych przyczyn powinny mieć możliwość dokumentowania zdarzeń i komunikacji z dyspozytorami. Mowa o pracownikach służb mundurowych, ale też tych pracujących w ochronie zdrowia lub zajmujących się ochroną dóbr wysokiej wartości. Myślę tu o ratownikach medycznych, komornikach sądowych, konwojentach czy operatorach bankowozów. Takie osoby z różnych względów mają potrzebę dokumentowania własnych działań, ale też tego, co dzieje się w ich otoczeniu. W wielu przypadkach zarówno dokumentacja, jak i możliwość wezwania wsparcia za pomocą tego samego urządzenia bywa dosłownie bezcenna. Przy czym kamera nie musi nagrywać cały czas. Poza specjalnymi sytuacjami, gdzie ewidencja musi być prowadzona w sposób ciągły, to operator decyduje, kiedy

uruchomić nagrywanie. Urządzenie zapisuje wówczas ostatnią minutę, od chwili włączenia zapisu. Podobnie działa przycisk SOS, który może wysłać zarówno naszą lokalizację, jak i rozpocząć transmisję na żywo dla naszego centrum operatorskiego.

W Polsce miało ostatnio miejsce kilka dramatycznych w skutkach ataków na personel medyczny. Czy według Pana sytuacja ta wpływa na zapotrzebowanie na nowoczesne rozwiązania bezpieczeństwa, takie jak kamery nasobne?

Podstawowa zasada jest taka, że ratownik powinien najpierw zadbać o swoje bezpieczeństwo, by móc pomóc poszkodowanym. Swoboda komunikacja z dyspozytorem, jaką zapewniają kamery nasobne Hytera oznacza, że ratownicy mogą liczyć na szybsze wsparcie innych służb. Taka komunikacja pozwala też na lepszą ocenę sytuacji, zarówno przed podjęciem akcji, jak i w jej trakcie. Równie istotny jest fakt, że kamera, w którą wyposażony jest ratownik, wpływa na emocje, często łagodząc obyczaje osób, które mają w stosunku do niego nie najlepsze zamiary. Nie bez znaczenia jest też to, że w uzasadnionych przypadkach nagrania z kamer nasobnych stanowią dowód na rzecz przyszłych potrzeb procesowych. •



ASBIS POLAND Sp. z o.o.

ul. Słowikowskiego 81C/bud. H4
05-090 Raszyn
sales@asbispoland.com



Czy stanie na stacji lokomotywa?



Po transformacji ustrojowej w 1989 roku polski transport kolejowy przeszedł głęboki kryzys, który doprowadził do znacznego ograniczenia sieci kolejowej i związanego z tym spadku liczby pasażerów. Obecnie, dzięki ambitnym planom inwestycyjnym, polska kolej ma szansę na renesans i odzyskanie swojej pozycji w systemie transportowym kraju.

Monika Żuber-Mamak

Trzy dekady temu polska kolej wkraczała w okres transformacji ustrojowej jako jeden z największych systemów w Europie. Długa na 26 tys. km sieć (jak w 1990 r. informował GUS) przewoziła blisko miliard pasażerów rocznie. Po torach mknęło 4 tys. lokomotyw i setki zespołów trakcyjnych. Dziś kolej stoi w obliczu zupełnie nowych wyzwań – od ograniczeń sieci po ambitne programy inwestycyjne, które mają przywrócić jej dawny blask.

Już w pierwszych latach po 1989 r. polskie koleje, nadal zmonopolizowane przez PKP, odczuły skutki deregulacji i kurczenia się przemysłu. W dekadzie 1990–2000 liczba pasażerów spadła o ponad 60%, z miliarda do 400 milionów rocznie (również dane GUS, choć z roku 2000), a sieć skurczyła się o 6,7 tys. km (tym razem wg raportu opublikowanego przez Urząd Transportu Kolejowego w 2023 r.). Wycofywano przestarzałe lokomotywy, a setki lokalnych linii przestały być eksploatowane.

I pełno ludzi w każdym wagonie

Jak po transformacji wyglądał polski transport publiczny? A w zasadzie jak wygląda w wielu miejscach do dziś? Mniej więcej tak:

– *Ja, to proszę pana, mam bardzo dobre połączenie. Wstaję rano, za piętnaście trzecia. Latem to już widno. Za piętnaście trzecia*



jestem ogolony, bo golę się wieczorem, śniadanie jadłem na kolację, więc tylko wstaję i wychodzę. (...) Idę do mleczarni, to jest godzinka. Potem szybko wiozą mnie do Szymanowa. Mleko, wiesz pan, ma najszybszy transport, inaczej się zsiada. W Szymanowie zsiadam, znoszę bańki i łapię EKD. Na Ochocie w elektryczny, do Stadionu. A potem to mam już z górki (...), bo tak: 119, przesiadka w trzynastkę, przesiadka w 345 i jestem w domu. To znaczy w robocie. I jest za piętnaście siódma. To jeszcze mam kwadrans. To jeszcze sobie obiad jem w bufecie. To po fajrancie już nie muszę zostawać, żeby jeść, tylko prosto do domu i góra 22.50 jestem z powrotem. (...)

To słynny fragment z filmu Stanisława Barei „Co mi zrobisz, jak mnie złapiesz”. Trochę na potrzeby artykułu skróciliśmy ten monolog. Wsie i miasteczka, nie tylko te Polski B, praktycznie zostały pozbawione transportu. Kto miał swój samochód, ten miał jak dotrzeć do pracy, lekarza albo do szkoły. Inni? Jechali z mlekiem. Albo wcale. Albo w wagonie, w którym jest naprawdę pełno ludzi. W 2022 r. portal Rynek Kolejowy opublikował kolejową mapę wstydu, która dobitnie pokazała, jakiej zapaści uległ transport kolejowy po 1989 r. (mapę można znaleźć na portalu Rynek Kolejowy w artykule „Tych połączeń już nie ma, czyli kolejowa mapa wstydu”).

Brak połączeń dotknął zwłaszcza mieszkańców Lubelszczyzny, Podkarpacia i Świętokrzyskiego. Według Polskiego Instytutu Ekonomicznego aż do dzisiaj ponad 13 mln (!) Polaków doświadcza wykluczenia transportowego, a w ponad 1200 gminach nie kursuje żaden transport publiczny. To nie tylko logistyczny kłopot czy chwilowa nieprzyjemność. Likwidacja wielu połączeń kolejowych doprowadziła do wykluczenia transportowego znacznej części społeczeństwa. Szczególnie poszkodowane są osoby mieszkające w małych miejscowościach, gdzie brak alternatywnych środków transportu publicznego utrudnia dostęp do pracy, edukacji i usług zdrowotnych.

A skądże to, jakże to? Ministerstwo informuje i alarmuje

W styczniu 2023 r. Ministerstwo Infrastruktury ujawniło alarmujące dane dotyczące dostępności kolei w Polsce. Ponad 400 polskich miast (dokładnie 408 ośrodków) było wówczas pozbawionych dostępu do transportu kolejowego, co stanowi 42% wszystkich miast w kraju. Informacje podane przez ministerstwo odnosiły się do stanu z początku 2022 roku. Transport autobusowy czy prywatne samochody nie były i w dalszym ciągu nie są w stanie załatać wyrwy, jaką pozostawiły po sobie puste torowiska.



Sieć kolejowa przez lata systematycznie się kurczyła – z prawie 24 tys. kilometrów eksploatowanych linii w 1990 r. spadła do około 19 tys. kilometrów w 2020 r. Najnowsze dane wskazują, że obecnie w eksploatacji jest 19 573 km torów (według informacji opublikowanych przez Independent Regulators' Group-Rail w najnowszym roczniku monitorującym stan transportu kolejowego w krajach należących do grupy. Polska jest jednym z 31 członków).

Wśród największych miast pozbawionych połączeń kolejowych znajdują się m.in. 85-tysięczne Jastrzębie-Zdrój (największe miasto w Polsce bez dostępu do kolei, ostatni pociąg odjechał z tamtejszego peronu w 2001 r.), prawie 65-tysięczne Siemianowice Śląskie, niespełna 61-tysięczna Łomża, 54-tysięczny Bełchatów czy prawie 31-tysięczne Police.

Według ministerstwa 4% z tych 408 miast powinno być obsługiwanych przez połączenia dalekobieżne, pozostałe miasta muszą liczyć na zapewnienie transportu kolejowego przez samorządy wojewódzkie w ramach przewozów regionalnych. Do wielu z wymienionych ośrodków pociągi mają powrócić w najbliższych latach dzięki programowi Kolej+ i innym inwestycjom infrastrukturalnym.

Lecz choćby przyszło tysiąc atletów...

...to i tak nie dałoby rady ukrytym kosztom likwidacji polskich linii kolejowych. Proces likwidacji połączeń kolejowych, a czasami wręcz fizycznej ich likwidacji, niesie ze sobą znacznie większe obciążenia finansowe, niż mogłoby się wydawać. Pozornie racjonalna decyzja o redukcji kosztów utrzymania nierentownych tras w rzeczywistości generuje szereg wydatków, które obciążają budżet państwa na lata.

JUŻ LEDWO SAPIE, JUŻ LEDWO ZIPIE

W latach 80. XX wieku polska sieć kolejowa liczyła około 26 000 km, a rocznie przewożono ponad miliard pasażerów. Po 1989 r. nastąpił gwałtowny spadek przewozów pasażerskich i towarowych. W okresie 1989-2004 sieć kolejowa w Polsce zmniejszyła się o 6 tys. km torów, a do 2019 r. o kolejnych 7 tys. km.

Przyczyny tego stanu rzeczy to m.in.

- **Niedoinwestowanie infrastruktury:**
Brak modernizacji torów i taboru doprowadził do spadku jakości usług.
- **Likwidacja nierentownych połączeń:**
Wiele lokalnych linii zostało zamkniętych, co ograniczyło dostępność kolei w mniejszych miejscowościach.
- **Konkurencja transportu drogowego:**
Rozwój sieci drogowej i wzrost liczby samochodów osobowych spowodowały odpływ pasażerów z kolei.



Bezpośrednie obciążenia finansowe

Demontaż infrastruktury kolejowej często kosztuje więcej niż przynosi zysków. PKP regularnie dopłaca do procesu rozbiórki torów, ponieważ przychody ze sprzedaży złomu nie pokrywają kosztów prac rozbiórkowych. Do tego dochodzą wydatki na rekultywację terenu, które dodatkowo obciążają budżet spółki i ostatecznie państwa.

Jednocześnie likwidacja linii kolejowych powoduje przeniesienie przewozów towarowych na transport drogowy, co skutkuje wzrostem kosztów logistycznych w całej gospodarce. Droższy transport ciężarowy, większe zużycie paliwa, wyższe opłaty drogowe oraz rosnąca emisja dwutlenku węgla to tylko część problemów. Dodatkowo intensyfikacja ruchu ciężarowego przyspiesza degradację dróg publicznych, co wymaga częstszych i kosztowniejszych remontów.

Konsekwencje dla rozwoju regionalnego

Gminy pozbawione dostępu do kolei tracą znaczące możliwości rozwojowe. Brak połączeń kolejowych obniża atrakcyjność inwestycyjną regionów, ogranicza rozwój turystyki i negatywnie wpływa na wartość nieruchomości. Ograniczona mobilność mieszkańców prowadzi do zjawiska depopulacji małych miast, co dodatkowo pogłębia problemy społeczno-ekonomiczne tych obszarów.



99

Według szacunków inwestycje mogą zwiększyć liczbę pasażerów z 370 mln rocznie do ponad 500 mln już w 2035 r., skracając czas podróży o 30–60% i obniżając emisję dwutlenku węgla w transporcie o 30% do 2040 r.

Zagrożenia dla bezpieczeństwa państwa

Rządowe analizy wskazują, że likwidacja linii kolejowych o znaczeniu strategicznym wymaga szczególnej oceny pod kątem obronności kraju. Utrata alternatywnych tras osłabia możliwości szybkiego przemieszczania wojsk czy transportu zaopatrzenia w sytuacjach kryzysowych. Zlikwidowane linie kolejowe nie mogą służyć jako zapasowe połączenia w przypadku awarii głównych szlaków komunikacyjnych.

Doświadczenia brytyjskie z lat 60. pokazują dramatyczne konsekwencje masowej likwidacji linii kolejowych. Kraj, który zdecydował się na radykalne cięcia w sieci kolejowej, musiał później ponosić ogromne koszty odbudowy infrastruktury, gdy okazało się, że system transportowy stał się niewydolny i nieelastyczny.

Utracone możliwości finansowania

Programy Unii Europejskiej, takie jak Polityka Spójności czy instrument CEF, oraz krajowe inicjatywy jak Kolej Plus czy Krajowy Program Kolejowy, przewidują znaczące środki na rewitalizację infrastruktury kolejowej. Likwidacja linii oznacza rezygnację z możliwości skorzystania z tych dotacji, co przekłada się na utracone korzyści ekonomiczne i społeczne na następne dekady.

Analiza rzeczywistych kosztów likwidacji linii kolejowych pokazuje, że pozorne oszczędności w krótkim okresie generują

znacznie większe wydatki w perspektywie długoterminowej. Każda decyzja o zamknięciu odcinka kolejowego powinna być poprzedzona gruntowną analizą uwzględniającą nie tylko bezpośrednie koszty utrzymania, ale także szersze konsekwencje gospodarcze, społeczne, ekologiczne i strategiczne. Tylko takie podejście pozwoli uniknąć kosztownych błędów, które obciążają gospodarkę i społeczeństwo przez dziesięciolecia.

I spieszy się, spieszy, by zdążyć na czas

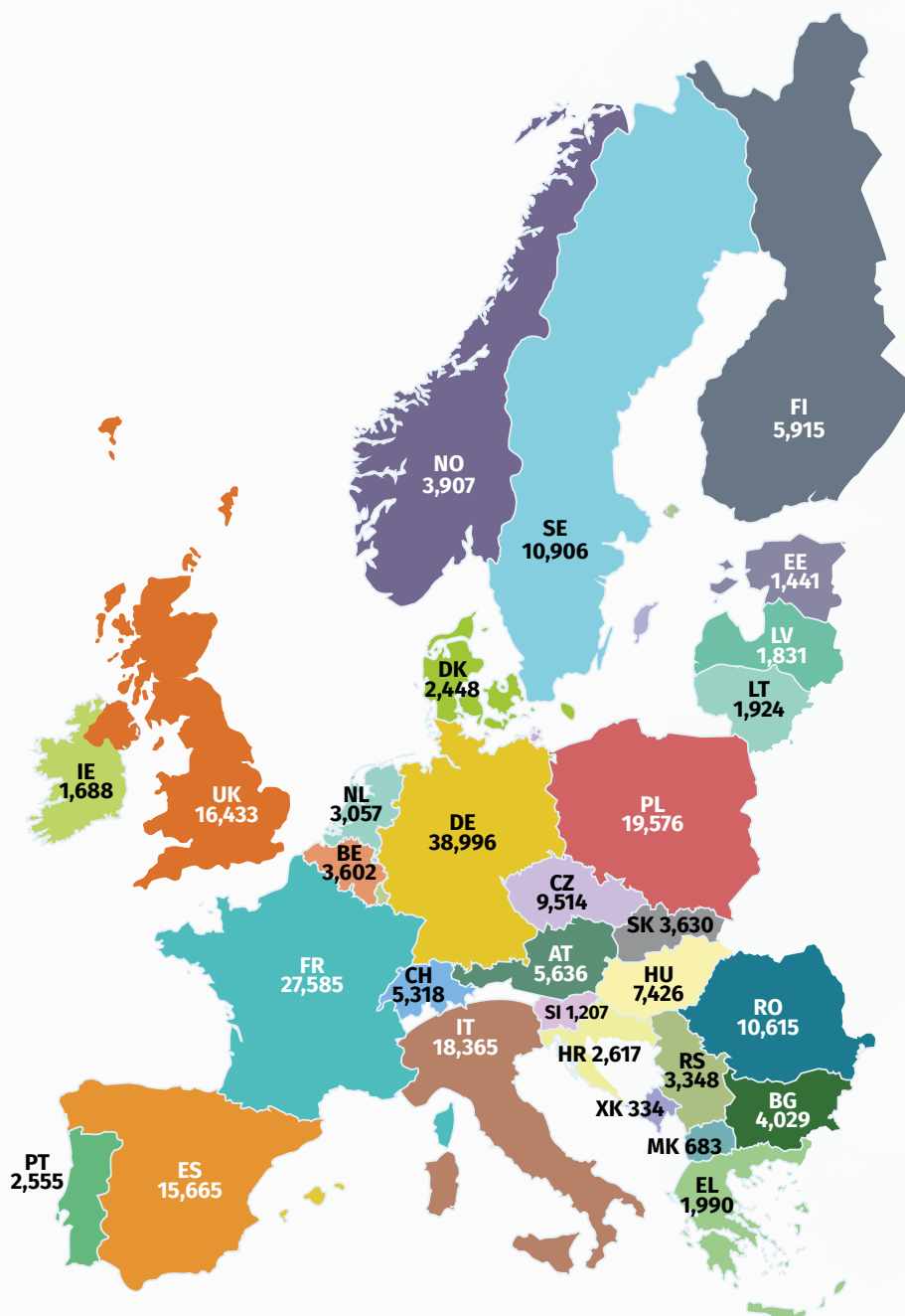
Podczas rządowej konferencji „Polska. Rok przełomu”, która odbyła się w lutym 2025 r., ogłoszone zostały bezprecedensowe plany inwestycyjne w infrastrukturę kolejową. Do 2032 r. na rozwój polskiej kolei zostanie przeznaczone 180 mld zł. Szef rządu podkreślił wówczas, że te inwestycje nie są jedynie planami na przyszłość – wiele z nich już zostało uruchomionych i są aktualnie realizowane.

Premier zaznaczył znaczenie inwestycji kolejowych nie tylko dla transportu pasażerskiego, ale również dla całej gospodarki. Rozbudowa sieci kolejowej ma umożliwić budowę pierwszej polskiej elektrowni atomowej oraz usprawnienie obsługi portów morskich. Donald Tusk zapowiedział również potrojenie przeładunków w polskich portach do 2030 r., co ma poprawić warunki dla rodzimych producentów i wzmocnić bezpieczeństwo gospodarcze kraju.

EUROPEJSKA SIEĆ KOLEJOWA

W 2023 r. łączna długość tras w krajach monitorowanych przez IRG-Rail wyniosła ponad 232 500 km. W ostatnich latach całkowita długość tras pozostaje w zasadzie jest stabilna. W poszczególnych krajach zaszły pewne zmiany (szczegóły znajdują się w dokumencie roboczym). Mogą występować zmiany w obrębie sieci, które nie są widoczne w danych, na przykład wtedy, gdy zamknięci linii zostały zrównoważone przez nowe inwestycje budowlane.

Prawie 70% całkowitej długości tras przypada na osiem krajów z największymi sieciami: Niemcy, Francję, Polskę, Włochy, Wielką Brytanię, Hiszpanię, Szwecję i Rumunię. Luksemburg posiada najkrótszą sieć spośród wszystkich uczestniczących krajów (271 km).



Środki na kolejnictwo zostaną rozdzielone w ramach sześciu kluczowych programów. Największą część – 79,1 mld zł – pochłonie Krajowy Program Kolejowy realizowany do 2030 r. (z możliwością przedłużenia do 2032 r.). Na drugim miejscu znajdują się inwestycje kolejowe związane z CPK – 75,1 mld zł. Program Kolej+ otrzyma 13,3 mld zł do 2029 r., a projekty finansowane z Krajowego Planu Odbudowy – 9,5 mld zł. Pozostałe środki przeznaczono na infrastrukturę towarzyszącą elektrowni jądrowej (2,8 mld zł) oraz modernizację przystanków kolejowych (0,3 mld zł w latach 2021-2025).

Według szacunków inwestycje mogą zwiększyć liczbę pasażerów z 370 mln rocznie do ponad 500 mln już w 2035 r., skracając czas podróży o 30–60% i obniżając emisję dwutlenku węgla w transporcie o 30% do 2040 r. (Strategia Zrównoważonego Rozwoju Transportu). Nowe połączenia KDP będą spoiwem

ekonomicznym między największymi ośrodkami, a CPK ma stać się „portem” usług logistycznych od Wisły do Bałtyku.

A dokąd? A dokąd? A dokąd? Na wprost! Czyli CPK i jego szprychy

Jednym z kluczowych projektów jest budowa Centralnego Portu Komunikacyjnego, który ma stać się węzłem przesiadkowym łączącym transport lotniczy, kolejowy i drogowy. W ramach CPK planowana jest budowa nowych linii kolejowych, które skrócą czas podróży między największymi miastami w Polsce.

W momencie powstawania niniejszego artykułu premier Donald Tusk ogłosił, że Centralny Port Komunikacyjny przechodzi w etap faktycznej realizacji. Premier zapowiedział rozpoczęcie kluczowego procesu przetargowego na głównego wykonawcę budowy terminala pasażerskiego lotniska CPK. Ta procedura, prowadzona



NAZWA PROGRAMU	OKRES REALIZACJI	PLANOWANY BUDŻET	OPIS PROGRAMU
Program Uzupełniania Lokalnej i Regionalnej Infrastruktury Kolejowej „Kolej +”	2019–2029	Na jego realizację przeznaczonych zostało ok. 13,2 mld zł. Z czego: ok. 11,2 mld zł pochodzić będzie z dokapitalizowania spółki PKP Polskie Linie Kolejowe SA; ok. 2 mld zł ma być wkładem własnym jednostek samorządu terytorialnego (np. obligacje, kredyty). Zadania inwestycyjne będą mogły być sfinansowane w maksymalnie 85% ze środków Programu, a w minimum 15% ze środków samorządowych.	Modernizacja i budowa lokalnych i regionalnych linii oraz przystanków w celu likwidacji wykluczenia komunikacyjnego. Reaktywacja połączeń w 34 lokalizacjach, w tym budowa nowych linii m.in. do Jastrzębia-Zdroju, Sremsu, Kozienic.
Krajowy Program Kolejowy (KPK)	2014–2030	Budżet na lata 2014–2030 wynosi 170 mld zł. Z tego, 79 mld zł to środki z perspektywy 2014–2020, 80 mld zł to środki z perspektywy 2021–2027, a 11 mld zł to środki z Krajowego Programu Odbudowy (KPO)	Kompleksowa modernizacja sieci bazowej (TEN-T), rozwój korytarzy towarowych oraz inwestycje punktowe na kluczowych odcinkach. W tym modernizacja 9000 km torów oraz elektryfikacja 1400 km. Poprawa przepustowości i bezpieczeństwa
Rządowy program wsparcia zadań zarządców infrastruktury kolejowej (utrzymanie i remonty)	do 2028 r.	W latach 2024–2028 ze środków publicznych założono łączny limit w wysokości 49 216,5 mln zł, w tym z budżetu państwa 44 005,4 mln zł	Finansowe wsparcie dla PKP PLK i innych zarządców infrastruktury na prace utrzymaniowe i remontowe torów oraz obiektów. Zapewnienie odpowiedniego poziomu jakości infrastruktury kolejowej, likwidacja zaległości utrzymaniowych, zachowanie sieci linii kolejowych oraz wieloletnie umowy na utrzymanie i remonty linii kolejowych.
Rządowy program budowy lub modernizacji przystanków kolejowych (tzw. program przystankowy)	2021–2025	Na ten cel przeznaczono 1 mld zł	Środki zostaną wykorzystane m.in. na wybudowanie lub zmodernizowanie przystanków kolejowych, a także sfinansowanie zadań związanych z dostępnością miejsc parkingowych dla podróżnych. Program obejmie przystanki kolejowe zlokalizowane w całej Polsce.
Program wsparcia dla kolei wąskotorowych (w przygotowaniu)	Prawdopodobnie od 2026 r.	Brak danych	Ministerstwo Infrastruktury pracuje nad zmianami prawnymi dotyczącymi funkcjonowania kolei wąskotorowych. Ma powstać fundusz, z którego przewoźnicy pozyskaliby środki na utrzymanie przewozów i infrastruktury. Dofinansowanie miałyby służyć rewitalizacji i utrzymania sieci kolei wąskotorowych.

w formie dialogu konkurencyjnego, kończy okres wieloletnich planów i rozpoczyna rzeczywiste działania budowlane.

Spółka CPK planuje w tym roku rozpiścić konkursy o łącznej wartości około 30 mld zł. Obejmą one nie tylko konstrukcję terminala lotniczego, ale także realizację pierwszej linii kolejowej wysokich prędkości (linia nr 85 w kształcie litery Y), która połączy stolicę z CPK i Łodzią.

Rząd wprowadził specjalne zasady postępowania przetargowego, które będą faworyzować polskie przedsiębiorstwa. Terminal lotniska ma kosztować około 5 mld zł.

Nowe lotnisko, położone między Warszawą a Łodzią, zostanie zaprojektowane z możliwością obsługi 34 mln podróżnych rocznie, z perspektywą elastycznego rozszerzania zgodnie z potrzebami rynku. Według harmonogramu prace budowlane rozpoczną się w 2026 r. na terenie gmin Baranów, Wiskitki i Teresin. Port ma

otrzymać certyfikaty w 2031 r. i zostać uruchomiony rok później wraz z pierwszym fragmentem kolei dużych prędkości. Całkowity koszt przedsięwzięcia do 2032 r. szacuje się na 131,7 mld zł.

Polska kolej stoi przed szansą na odzyskanie swojej pozycji jako kluczowego elementu systemu transportowego kraju. Dzięki ambitnym planom inwestycyjnym i modernizacji infrastruktury kolej może stać się atrakcyjną alternatywą dla transportu drogowego, przyczyniając się do zrównoważonego rozwoju i poprawy jakości życia obywateli. I nie trzeba już będzie jechać z mlekiem. Wystarczy wsiąść do pociągu.

Tak to to, tak to to, tak to to, tak to to!... •

W śródtytułach wykorzystane zostały fragmenty wiersza *Lokomotywa* Juliana Tuwima



Sabotaż na talerzu?

Żywność jako broń XXI wieku

Bezpieczeństwo żywności to temat, który ma kilka ważnych aspektów i warto na nie spojrzeć, biorąc pod uwagę różne perspektywy. Począwszy od rozważań na temat kondycji rodzimego rolnictwa i jego możliwości zaspokajania potrzeb ludności, przez łańcuch dostaw produktów żywnościowych, po kategorię bezpieczeństwa żywności i osób mających z tą żywnością kontakt.

Jacek Tyburek





Każdy z wymienionych etapów to osobny obszar badawczy, każdy z nich generuje inne wyzwania związane z bezpieczeństwem. Wynika to z jak zwykle niejednoznaczności pojęcia bezpieczeństwa. Dla jednych bezpieczeństwo oznacza zasady BHP, dla innych to bezpieczeństwo operacyjne, a jeszcze inaczej rozumieją je osoby z IT, którym bezpieczeństwo kojarzyć się będzie głównie z cyberbezpieczeństwem. Dokładnie tak samo wygląda kwestia pojmowania bezpieczeństwa żywności. Każdy tę kwestię może definiować inaczej, ale niezależnie od tego wszystkim ludziom zajmującym się tym tematem chodzić będzie o dobrostan i bezpieczeństwo konsumenta.

Co grozi bezpieczeństwu żywności

Po pierwsze, nieintencjonalne zanieczyszczenie lub spowodowanie znaczących wad w procesie produkcji żywności. Ta sfera regulowana jest przez system HACCP (*Hazard Analysis and Critical Control Points*) i związane z nim regulacje. Po drugie, działania celowe, np. próby zatrucia żywności. Nawet jeśli rzadko spotykane, to siła rażenia takiego działania może być ogromna.

W świecie definicji bezpieczeństwa żywnościowego

Aby móc rozmawiać o bezpieczeństwie żywności, rozpocząć należy od określenia trzech różnych perspektyw rozpatrywania bezpieczeństwa obywateli w kontekście żywności:

1. Bezpieczeństwo żywności wg FAO (Food and Agriculture Organization of the United Nations – Organizacja Narodów Zjednoczonych do spraw Wyżywienia i Rolnictwa) oznacza pewność, że nie spowoduje ona szkody dla konsumenta, gdy jest przygotowywana i/lub spożywana zgodnie z przeznaczeniem.

2. Bezpieczeństwo żywności (food safety) – ogół koniecznych do spełnienia warunków i działań, które muszą być podjęte podczas wszystkich etapów procesu produkcji żywności i obrotu handlowego żywnością w celu zapewnienia bezpieczeństwa życia i zdrowia konsumentów.

3. Food defence – pojęcie, które na stałe wpisało się do systemów zarządzania bezpieczeństwem żywności. Oznacza ono ochronę produktów żywnościowych przed ich celowym skażeniem czynnikami fizycznymi, chemicznymi, biologicznymi lub radiologicznymi.

Wspomniany wcześniej HACCP jest systemem analizy zagrożeń i krytycznych punktów kontroli. Oznacza to postępowanie ukierunkowane na zapewnienie bezpieczeństwa żywności. Celem jego wdrożenia jest wyeliminowanie lub redukcja do akceptowalnego poziomu wszystkich potencjalnych zagrożeń zdrowotnych związanych z produkcją i dystrybucją żywności, mogących się pojawić na poszczególnych etapach procesu produkcji, poczynawszy od dostawy surowców spożywczych, poprzez ich przechowywanie, przetwarzanie żywności, skończywszy na dystrybucji gotowych produktów i posiłków.

Na każdym z etapów system przedstawia rekomendacje działania, które jako najlepsze praktyki przedsiębiorca winien jest wdrożyć do bieżącej praktyki przedsiębiorstwa.

HACCP wymaga przypisania każdemu zidentyfikowanemu zagrożeniu tzw. środków kontroli, czyli działań, jakie muszą być podejmowane w celu opanowania tych zagrożeń. W wyniku identyfikacji, oceny istotności zagrożeń oraz prawdopodobieństwa ich wystąpienia wyznacza się tzw. krytyczne punkty kontroli (*Critical Control Point*, CCP), czyli miejsca w procesie, które z punktu widzenia skutecznego zapewnienia bezpieczeństwa żywności w zakładzie powinny znaleźć się pod szczególnym nadzorem.

Wymienione w punktach 2. i 3. *food safety* i *food defence* wiążą się bezpośrednio z możliwością zagrożenia terrorystycznego. Definicja bezpieczeństwa żywności, wraz z regulacjami HACCP, nie zakłada bowiem celowego zatrucia żywności, a jedyną okoliczność, której procesy HACCP mają zapobiegać, jest zjawisko falsyfikacji żywności w celu osiągnięcia korzyści. Temat bezpieczeństwa żywności pod względem jej ochrony w kontekście zagrożeń terrorystycznych jest nieobecny w ustawodawstwie polskim i europejskim. Jedyne regulacje, które istnieją, dotyczą ochrony tzw. infrastruktury krytycznej, w tym zapewniającej dostawę żywności i wody. Najbardziej w tym względzie rozwiniętym prawem na świecie jest amerykańskie prawo żywnościowe, w tym tzw. ustawa modernizacyjna, nakładająca obowiązek wdrożenia przez organizacje systemu analizy zagrożeń i opartych na ryzyku środków zapobiegawczych wobec żywności (*Hazard Analysis and Risk-Based Preventive Controls*, HARPC).

Pojęcie *food defence*, czyli obrony żywności, również w samych USA, pojawiło się na poważnie w następstwie ataków 11 września na World Trade Center w Nowym Jorku. Po tym zdarzeniu powołano zintegrowane „ministerstwo bezpieczeństwa wewnętrznego” – DHS – Department of Homeland Security. Doszło wtedy do licznych wydarzeń o charakterze bioterrorystycznym z wykorzystaniem laserek węglika, które spowodowały śmierć lub zagrożenie życia u blisko 30 osób. Od tego czasu w Stanach Zjednoczonych, by chronić żywność i łańcuch dostaw żywności, wprowadzono pojęcie obrony żywności, czyli jej ochrony przed celowym skażeniem.

Terroryzm żywnościowy jest aktem, w którym produkty spożywcze są wykorzystywane jako broń w walce z przeciwnikiem. Celem tego działania jest wywołanie konkretnych skutków społecznych poprzez zastraszanie atakowanej społeczności, w tym wywoływanie ataków paniki podsycane dodatkowo przez stosowne kampanie w mediach społecznościowych.

Ze względu na źródła czynników oraz metody wykorzystywane w terroryzmie żywnościowym można wskazać na jego różne odmiany, m.in.:

- **terroryzm biologiczny (bioterroryzm)**, który w przypadku żywności będzie oznaczać zamierzone skażenie produktów spożywczych i wody wirusami, bakteriami lub innymi drobnoustrojami w celu wywołania chorób lub uśmiercenia ludzi bądź zwierząt;
- **terroryzm chemiczny** prowadzony wobec łańcucha żywności z użyciem środków chemicznych, np. pestycydów.
- **terroryzm radiologiczny** z użyciem środków promieniotwórczych;
- **terroryzm fizyczny** czyli intencyjne wprowadzenie do żywności i jej łańcucha różnych zanieczyszczeń o charakterze fizycznym (ciał stałych, np. igieł, szkła, odłamków metalu);



- **agroterroryzm**, czyli czyn terrorystyczny wymierzony w tzw. produkcję podstawową, przez którą, zgodnie z rozporządzeniem (WE) 178/2002, rozumie się „produkcję, uprawę lub hodowlę produktów podstawowych, w tym zbiory, dojenie i hodowlę zwierząt gospodarskich przed ubojem; produkcja podstawowa oznacza także łowiectwo i rybołówstwo oraz zbieranie runa leśnego”.

Duże skupiska ludzi są łatwym celem

To zrozumiałe, że wszelkie akty terrorystyczne żywnościowego wymiaru będą raczej w duże skupiska ludzi, mówiąc wprost – w mieszkańców miast. Dlatego władze municypalne powinny mieć przygotowane plany działań na wypadek takiej sytuacji. Jednak przygotowanie takiego planu wymaga prawidłowego rozpoznania możliwości prawnych lokalnych oraz szerzej prawa krajowego i w przypadku dużego polskiego miasta regulacji Unii Europejskiej. Po raz kolejny należy zaznaczyć, że zasługi powstania i wdrożenia systemu HACCP są nie do przecenienia. Powstanie tej metodologii, regulacji prawnych ją regulujących i zabezpieczających oraz całego systemu kontroli bezpieczeństwa żywności dało niezbędną podstawę do zapewniania skuteczności procesu bezpieczeństwa żywności.

Dokument taki powinien zawierać rekomendacje, metody działania oraz organizację na akty terroru poprzez żywność. Pojęcie i odwołanie do konieczności wdrożenia obrony żywności, w rozumieniu środków, wysiłków, działań związanych z ochroną żywności i podmiotów ją wytwarzających, nie występuje w unijnym prawie żywnościowym ani tym bardziej w prawie polskim.

W Europie funkcjonuje wiele przepisów i standardów pomocnych w zapobieganiu terroryzmowi związanemu z żywnością. Działania te koncentrują się na zapewnieniu bezpieczeństwa łańcucha dostaw żywności, wykrywaniu zagrożeń oraz reagowaniu w przypadku ich pojawienia się. Obowiązujące obecnie akty prawne to:

- **rozporządzenie (WE) nr 178/2002** Parlamentu Europejskiego i Rady;
- **rozporządzenie wykonawcze Komisji (UE) NR 931/2011** w sprawie wymogów dotyczących możliwości śledzenia ustanowionych rozporządzeniem (WE) nr 178/2002 Parlamentu Europejskiego i Rady w odniesieniu do żywności pochodzenia zwierzęcego;
- **rozporządzenie (WE) nr 852/2004** w sprawie higieny żywności;
- **rozporządzenie (WE) nr 1935/2004** Parlamentu Europejskiego i Rady z dnia 27 października 2004 r. w sprawie materiałów i wyrobów przeznaczonych do kontaktu z żywnością;
- **rozporządzenie (WE) nr 1069/2009** z dnia 21 października 2009 r. określające przepisy sanitarne dotyczące produktów ubocznych pochodzenia zwierzęcego, nieprzeznaczonych do spożycia przez ludzi;
- **zasady i wytyczne Europejskiego Urzędu ds. Bezpieczeństwa Żywności (EFSA);**
- **Ustawa o bezpieczeństwie żywności i żywienia** (Dz.U. 2006 nr 171 poz. 1225);
- **dyrektywa 2008/114/WE** w sprawie identyfikacji infrastruktury krytycznej.

Nie są to jednak przepisy odnoszące się wprost do zagadnienia obrony, prewencji i działania w sytuacji kryzysowej w związku

z atakiem terrorystycznym poprzez żywność. Znacznie bardziej zaawansowana w kwestii regulacji bezpieczeństwa obrony żywności właśnie jest administracja USA.

Planowanie działań na rzecz obrony żywności zgodnie z wytycznymi Departament Rolnictwa Stanów Zjednoczonych (United States Department of Agriculture, USDA) ma na celu przede wszystkim rozpoznanie przyszłości, a także zmniejszenie ryzyka wystąpienia danego zdarzenia (wydarzenia, negatywnego przypadku, sytuacji kryzysowej). Służy też ograniczeniu powstania chaosu i paniki, co ma zapobiegać eskalacji niebezpiecznej sytuacji. Plan obrony żywności przygotowany zgodnie z wytycznymi USDA to dokument określający środki kontroli podejmowane przez zakład celem ochrony żywności przed jej intencyjnym zanieczyszczeniem. Plan tego typu powinien być opracowany i zapisany, wprowadzony do praktyki, przetestowany, czyli sprawdzony, pod kątem poprawności i skuteczności, a następnie wdrożony i utrzymywany. Co więcej, charakter takiego planu zależy od specyfiki przedsiębiorstwa, a to oznacza, że ogólne i bardzo lakoniczne założenia zawarte w rozporządzeniu w sprawie planów ochrony infrastruktury krytycznej mogą nie być wystarczające, by stworzyć skuteczny plan obrony żywności. Krajowe wymagania odnoszą się bowiem do tego, jakie obszary organizacji powinny być zabezpieczone, nie wyznaczając jednocześnie konkretnych rozwiązań.

Zatem ani prawo żywnościowe, ani prawo mające zastosowanie w sytuacji kryzysowej nie tworzy właściwych warunków do stosownej obrony żywności w tym zakresie. Byłoby tak,



gdyby w ślad za wymogami prawa stosowne urzędy przygotowały jeszcze zbiór wytycznych zalecanych do wykorzystania przez poszczególne przedsiębiorstwa. Dodać bowiem należy, że USDA stworzył wiele sprzyjających warunków organizacjom przemysłu spożywczego, by opracowały skuteczny plan obrony żywności. Przykładem jest możliwość skorzystania z narzędzia o nazwie *Food Defense Plan Builder* (FDPB) w wersji 2.0, którego zastosowanie, choć fakultatywne, ma przede wszystkim pomóc organizacjom spożywczym wywiązać się z ciążącego na nich obowiązku spełnienia wymagań ustawy modernizacyjnej bezpieczeństwa żywności FSMA (*Food Safety Modernization Act*) *Final Rule for Mitigation Strategies to Protect Food Against Intentional Adulteration*, podpisanej przez prezydenta Stanów Zjednoczonych 4 stycznia 2011 r. Ważną rolę w tej ustawie spełnia bowiem system analizy zagrożeń i opartych na ryzyku środków zapobiegawczych wobec żywności (*Hazard Analysis and Risk-Based Preventive Controls*, HARPC), wzorowany na systemie HACCP.

Wśród wielu wymagań cytowanej ustawy pojawił się obowiązek, aby producenci żywności opracowali szeroko rozumiane plany bezpieczeństwa żywności, uwzględniające różne możliwe rodzaje zagrożeń, w tym celowe zanieczyszczenie żywności. Rolą tego systemu jest ochrona produktu i konsumenta przed

zagrożeniami nieprzypadkowymi (celowymi) i przypadkowymi, w tym powstałymi wskutek terroryzmu żywnościowego i zafałszowań żywności. Wymagania zawarte w ustawie obowiązują nie tylko organizacje amerykańskie. Mają zastosowanie wobec wszystkich dostawców produktów żywności na rynek USA. System HARPC dotyczy zatem także organizacji ulokowanych w naszym kraju. Z zasad systemu HARPC zostały jednak wyłączone następujące grupy produktów: soki i świeże owoce morza (podlegające indywidualnej ocenie ryzyka wg systemu HACCP), napoje alkoholowe, a także żywe zwierzęta, mięso, drób i jaja (podlegające wymaganiom USDA).

Obowiązujące w Europie podejście różni się od podejścia modelu *food defence* obowiązującego w USA. Model amerykański przewiduje budowanie szczelnego systemu obrony żywności z użyciem tych samych reguł i narzędzi, które wykorzystywane są do ochrony produktów i obiektów zaliczanych do infrastruktury krytycznej. To oznacza, że przemysł spożywczy musi dokonywać w zasadzie takich samych inwestycji w urządzenia techniczne, przygotowanie służby ochrony, budowanie świadomości pracowników zajmujących się żywnością na każdym etapie łańcucha dostaw, jak firmy, które uznane zostały za ważne dla infrastruktury krytycznej. •

Elementy konieczne do stworzenia planu bezpieczeństwa żywnościowego miasta:

Charakterystyka (analiza socjologiczna)	Współczesne trendy i praktyki budowania łańcuchów dostaw żywności dla miast	Mapowanie systemów dystrybucji żywności zgodnie z zasadą „od rolnika do konsumenta”	Przygotowanie zestawienia uczestników i punktów dystrybucji żywności w mieście
Przygotowanie wstępnej analizy ryzyka dla zagrożeń mieszkańców miast	Szacowanie (na bazie analizy ryzyka) najbardziej prawdopodobnych zagrożeń (lub takich o najpoważniejszych skutkach)	Zestawienie dobrych praktyk, rekomendacji oraz standardów zapewnienia bezpieczeństwa żywności w mieście	Typologia i zestawienie krytycznych elementów systemów bezpieczeństwa żywnościowego
„Mała” gra decyzyjna	Zarysy procesów bezpieczeństwa żywności w ramach systemu miejskiego	Przygotowanie ramowej konstrukcji Polityki Bezpieczeństwa Żywnościowego Miasta	Pełnoskalowa gra decyzyjna
SWOT	Edukacja	Media społecznościowe	Przygotowanie wydawnictw skierowanych do interesariuszy



Jacek Tyburek

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



Głos branży

Bezpieczeństwo publiczne to fundament sprawnie funkcjonującego społeczeństwa. Obejmuje działania mające na celu ochronę życia, zdrowia i mienia obywateli przed zagrożeniami takimi jak przestępczość, katastrofy naturalne czy wypadki. Zapewnienie bezpieczeństwa to zadanie nie tylko służb mundurowych – policji, straży pożarnej, ratownictwa – ale również samorządów, instytucji państwowych i każdego z nas.

Czas na odpowiedzialne decyzje

ARTUR HEJDYSZ
C&C PARTNERS



Nie mogę się doczekać czasów, w których każdy inwestor, zarówno publiczny, jak i prywatny, będzie świadomie zarządzał ryzykiem przy realizacji projektów z zakresu bezpieczeństwa. Przez wiele lat systemy zabezpieczeń traktowano po prostu jako spełnienie biurokratycznych wygań i zadośćuczynienie formalnościom. Tymczasem w dobie rosnących zagrożeń, także tych cyfrowych, potrzebujemy jakości, nie pozorów.

Mam nadzieję, że nowe regulacje, zwłaszcza te zawarte w ustawie o krajowym systemie cyberbezpieczeństwa, wymuszą zmianę podejścia. Nie możemy dłużej pozwalać na zakup urządzeń

z niepewnych źródeł, które zamiast chronić, same mogą być zagrożeniem. Systemy bezpieczeństwa nie mogą być wybierane według klucza „najniższa cena”.

Ważne jest korzystanie z rozwiązań pochodzących od zweryfikowanych producentów i dostawców – takich, którzy nie tylko oferują produkty o sprawdzonym pochodzeniu, ale też posiadają odpowiednie certyfikaty. Z mojego doświadczenia wynika, że można znaleźć firmy, które spełniają najwyższe standardy bezpieczeństwa, a jednocześnie nie odbiegają cenowo od rynkowej średniej.

Zbyt wielu inwestorów postrzega dziś przepisy ustawy Prawo zamówień publicznych jako barierę, która ogranicza ich możliwości. Tymczasem to właśnie w ich interesie leży, by domagać się dowodów pochodzenia produktów, certyfikatów zgodności czy potwierdzenia kompetencji instalatorów. Przecież nikt nie chce, aby systemy bezpieczeństwa były instalowane przez osoby lub firmy, które same mogą stanowić potencjalne ryzyko.

Czas na świadome, odpowiedzialne decyzje. Bezpieczeństwo nie może być kompromisem. •

Bezpieczna uczelnia

ANETA SADACH

Uniwersytet Łódzki,
Wydział Filologiczny



Wiem, że ostatnie tragiczne wydarzenia na Uniwersytecie Warszawskim wywołały duże poruszenie, nie tylko wśród społeczności akademickiej. Nielatwo jest zadbać o bezpieczeństwo miejsc publicznych, szczególnie takich, jak uczelnie czy kampusy, pełnych ludzi wchodzących i wychodzących, ale też odpoczywających na korytarzu czy na terenie zewnętrzym budynków. Takie są m.in. kampusy i budynki uczelni wyższych. I nie można ich zamknąć. To specyfika takich miejsc – uczelnie są otwarte dla studentów i przyszłych studentów, pracowników, stażystów. Uczynienie twierdzy z uczelni nie jest oczywiście niemożliwe, ale przecież nie o to chodzi.

Niestety, nie da się zapobiec wszystkim zagrożeniom. Można natomiast je minimalizować, próbować ograniczyć ryzyko wypadków czy czynów wprost wymierzonych przeciwko zdrowiu bądź życiu osób przebywających w danym miejscu. Dlatego już jakiś czas temu rozpoczęliśmy działania mające na celu automatyzację budynku polegającą na instalacji systemu kontroli dostępu, by chronił osoby przebywające na uczelni, ale nie utrudniał nam wszystkim pracy, likwidacji nieszczęsnego systemu wydawania kluczy, ochronę pomieszczeń strategicznych oraz specjalistycznych sal dydaktycznych z wyposażeniem o dużej wartości, np. studio TV, studio radiowe, pracownie komputerowe oraz kontrolę autoryzacji wjazdu na teren parkingu.

Wdrożony system kontroli dostępu to kluczowy element bezpieczeństwa naszego wydziału. Każdy pracownik dysponuje spersonalizowaną kartą elektronicznego dostępu. Karta upoważnia do korzystania z pomieszczeń zgodnie z przyznanymi uprawnieniami wynikającymi z charakteru pracy danego pracownika wydziału, pracownika serwisu lub najemcy zgodnie z zapisami umowy.

Dzięki zainstalowanym czytnikom elektronicznym studenci mogą skorzystać z sali pracy indywidualnej zgodnie z przesłanym wnioskiem. System obejmuje ponad 200 różnych pomieszczeń – od sal dydaktycznych, przez laboratoria językowe, pracownie komputerowe, aule, aż po sale specjalistyczne, szczególnie chronione. Dostęp do przestrzeni parkingowej odbywa się automatycznie za pomocą kamery LPR po autoryzacji wniosku. Dzięki takiemu rozwiązaniu minimalizujemy ryzyko wjazdu osoby nieuprawnionej. Integracja z kamerami monitoringu wizyjnego pozwala nam w czasie rzeczywistym na wykrycie tego, że na wydziale przebywają osoby nieuprawnione, oraz skutecznie reagować na incydenty.

W kolejnym etapie planujemy połączyć kontrolę dostępu z systemami alarmowym i sygnalizacji pożarowej, a także automatyką budynkową – od wentylacji po sterowanie oświetleniem budynku oraz terenu zewnętrznego. Zastosowane elementy bezpieczeństwa posłużą jednocześnie optymalizacji zużycia energii i zarządzaniu infrastrukturą. System jest programowalny i skalowalny – nowe urządzenia IoT mogą być w prosty sposób dołączane do istniejącej sieci. Dzięki temu jesteśmy gotowi na przyszłe wyzwania, od rozbudowy uczelni po integrację z miejskim monitoringiem i systemami ratowniczymi.

Po doświadczeniach z Warszawy wiemy, że takie kompleksowo rozwiązania, łączące fizyczne zabezpieczenia i inteligentne narzędzia informatyczne, mają realny wpływ na ludzkie życie. •

Bielsko-Biała pod okiem kamer

KRYSTIAN KOWALCZYK

Straż Miejska, Bielsko-Biała



Bielsko-Biała nie należy do czołówki największych miast, ale zdecydowanie wyróżnia się bogatym kalendarzem wydarzeń – kulturalnych, sportowych i społecznych – które nadają mu wyjątkową energię i charakter.

Sz szczególnie w sezonie letnim miasto tętni życiem, przyciągając licznych turystów, którzy chętnie korzystają z malowniczych tras rowerowych w Beskidach – w tym z popularnej sieci jednokierunkowych ścieżek Enduro Trails. Właśnie dlatego monitoring miejski odgrywa tak istotną rolę w codziennym zabezpieczeniu przestrzeni publicznej.

System ten sprawdza się w praktyce – czego dowodzi przykład z ostatnich dni. 23 kwietnia 2025 r. operator monitoringu zauważył akt wandalizmu na siłowni plenerowej przy placu Fabrycznym. Szybka reakcja i powiadomienie patrolu umożliwiły natychmiastowe ujęcie sprawcy. Choć nie było to zdarzenie spektakularne,

to właśnie takie codzienne interwencje budują realne poczucie bezpieczeństwa wśród mieszkańców.

Obecnie w systemie monitoringu wizyjnego miasta Bielska-Białej zainstalowane są 133 kamery stacjonarne oraz 1 kamera mobilna. Kamery stacjonarne rozmieszczone są w niewygodnych punktach, takich jak skrzyżowania, place czy obszary rekreacyjne. Dwie z tych kamer, zlokalizowane przy ul. Bohaterów Warszawy oraz placu Fabrycznym, zostały sfinansowane ze środków budżetu obywatelskiego, co świadczy o zaangażowaniu mieszkańców w poprawę bezpieczeństwa.

Współpraca z Miejskim Zarządem Dróg (MZD) pozwala na integrację systemu monitoringu z Systemem Zarządzania Ruchem (ITS), co umożliwia efektywne zarządzanie sygnalizacją świetlną na kluczowych skrzyżowaniach oraz szybką reakcję na incydenty drogowe. Na podstawie porozumienia z MZD tutejsza jednostka wykorzystuje 185 kamer stanowiących część Inteligentnego Systemu Transportowego. Dzięki temu możliwe jest nie tylko monitorowanie sytuacji na drogach, ale również natychmiastowe kierowanie patroli w rejon zagrożony.

Wykorzystujemy również analizę wideo opartą na algorytmach sztucznej inteligencji. Mimo imponujących możliwości, jakie oferuje AI, nie jest ona wolna od ograniczeń. Systemy te operują na podstawie danych i wzorców wcześniej im dostarczonych, co oznacza, że mogą błędnie zinterpretować niewinne



zachowanie jako zagrożenie – np. gwałtowną gestykulację podczas rozmowy jako agresję – lub zignorować subtelne sygnały niebezpieczeństwa, które człowiek rozpoznałby natychmiast.

Ponadto AI nie ma kontekstu kulturowego ani emocjonalnego, przez co jej oceny są chłodne i zero-jedynkowe. To może prowadzić do fałszywych alarmów lub przeoczeń, szczególnie w złożonych sytuacjach społecznych. Dlatego człowiek – operator monitoringu – pozostaje najważniejszym ogniwem w tym systemie. To on podejmuje ostateczne decyzje, ocenia kontekst i interpretuje sytuacje, których maszyna jeszcze nie potrafi w pełni zrozumieć. Z tego powodu sztuczna inteligencja wykorzystywana jest w systemie monitoringu wizyjnego miasta Bielska-Białej w ograniczonym zakresie. W oparciu o funkcje wykrywania podejrzanego zachowania monitorowane są m.in. ustronne miejsca, takie jak przejścia podziemne.

Analiza obrazu dla miast

NATALIA JAŚTAK
BCS



Miejski monitoring wizyjny odgrywa kluczową rolę w zapewnianiu porządku publicznego, umożliwiając m.in. natychmiastową reakcję na różne niebezpieczne zdarzenia. Coraz więcej samorządów sięga po nowoczesne rozwiązania wspierane uczeniem maszynowym i komputerowym przetwarzaniem obrazów, które pozwalają działać szybciej i skuteczniej.

Powszechnie są już stosowane funkcje wykrywające zamaskowane osoby, bagaże pozostawione bez opieki czy przejazdy na czerwonym świetle. Wczesne wykrywanie zagrożeń ma istotne znaczenie w kontekście prewencji. Funkcje te pozwalają jedynie na wykrycie zdarzenia, jednak nie ułatwiają dalszego poszukiwania osób czy pojazdów biorących w nim udział. Co powoduje, że ujęcie osób zamieszanych w dany incydent jest w zasadzie nie możliwe.

Innowacyjnym podejściem do analizy obrazu jest zautomatyzowane wyszukiwanie osób podejrzanych lub ich środków transportu (samochód, motor rower itd.). Tradycyjne metody przeszukiwania materiałów z kamer wymagają przeglądania kolejnych nagrań przez człowieka, czasami przez wiele godzin. Zautomatyzowane wyszukiwanie eliminuje ten problem. Wykorzystując nową technologię wyszukiwania, wystarczy zaznaczyć poszukiwany obiekt (sylwetkę osoby, pojazd, itd.) na podglądzie na żywo lub nagraniu. Wystarczy kolor koszulki, spodni, fryzura czy inny specyficzny element ubioru, aby system rozpoczął przeszukiwanie nagrań z zadanego przedziału czasowego. Analogicznie można wyszukiwać pojazdy na podstawie zapamiętanego przez obserwatora koloru, modelu czy kilku cyfr rejestracji pojazdu. Jeśli świadkowie mają zdjęcie poszukiwanego obiektu, również można je wykorzystać. Podczas wyszukiwania algorytm analizuje cechy fizyczne obiektu, porównując je z materiałami wideo z wielu kamer, a następnie na podstawie wyznaczonego

Obsługę i obserwację obrazu z kamer prowadzą wykwalifikowani operatorzy monitoringu. Zatrudniamy zarówno osoby z doświadczeniem w służbach porządkowych, jak i kandydatów, którzy – posiadając odpowiednie predyspozycje – zdobywają niezbędne kompetencje w trakcie szkoleń.

Warto podkreślić, że praca operatorów monitoringu miejskiego nie należy do łatwych – jest wymagająca, obciążająca psychicznie i nie każdy decyduje się ją podjąć. Z tego powodu zmagamy się z pewnymi brakami kadrowymi. Dlatego intensywnie poszukujemy nowoczesnych rozwiązań opartych na sztucznej inteligencji, które mogłyby realnie wesprzeć pracę człowieka – nie ją zastąpić. Nieustannie dążymy do stworzenia systemu skutecznego, niezawodnego i w pełni dostosowanego do miejskich realiów. •

poziomu ufności minimalizuje ryzyko błędów i zwraca podobne obrazy. Cały proces zajmuje kilka sekund, a operator systemów monitoringu otrzymuje już wstępnie wyfiltrowane nagrania. To pozwala znacznie szybciej lokalizować osoby i zdarzenia, które wymagają interwencji i daje ogromną przewagę w sytuacjach zagrożenia – pozwala błyskawicznie reagować na działania przestępcze, zwiększając bezpieczeństwo mieszkańców.

Technologia zautomatyzowanego wyszukiwania umożliwia również poszukiwanie osób czy pojazdów jedynie na podstawie relacji świadków. Zautomatyzowane wyszukiwanie działa skutecznie nawet w skomplikowanych, miejskich środowiskach – w tłumie ludzi, przy słabym oświetleniu czy w dynamicznych scenach.

Zautomatyzowane wyszukiwanie stanowi przyszłość dla systemów monitoringu miejskiego, wypierając proste analizy obrazu. Szybka, precyzyjna i dostępna zarówno dla dużych aglomeracji, jak i mniejszych przedmiotów technologia ułatwia działanie służb oraz daje realne poczucie bezpieczeństwa mieszkańcom. •



Zadbaj o cyberbezpieczeństwo wodociągów

DANIEL KAMIŃSKI
Orange



Zakłócenia w dostawie wody, skażenie jej jakości, a nawet całkowite unieruchomienie systemów sterowania przemysłowego (ICS/OT) mogą być spowodowane atakiem hakerskim na wodociągi. Konsekwencję odczują przede wszystkim mieszkańcy regionu, który jest obsługiwany przez zaatakowane przedsiębiorstwo wodociągowe.

W ostatnim czasie nastąpił wzrost cyberataków na infrastrukturę wodociągowo-kanalizacyjną. Odnotowano m.in. incydenty

w Kuźnicy, Tolkmicku, Małdytach i Sierakowie. Ataki miały realny wpływ na funkcjonowanie systemów, a ich skutki odczuli właśnie odbiorcy usług. Takie incydenty pokazują, jak ważna jest skuteczna ochrona infrastruktury tego typu.

Istotne stało się wdrożenie systemów wykrywania włamań (IDS) monitorujących ruch sieciowy i identyfikujących podejrzaną aktywność. Warto też skorzystać z możliwości operacyjnych centrów bezpieczeństwa (SOC OT), które zapewniają kompleksową analizę zagrożeń i szybką reakcję na incydenty. Integracja obu tych rozwiązań pozwala na skuteczne wykrywanie i neutralizowanie cyberataków i minimalizuje ryzyko zakłóceń w dostawie wody.

Ochrona wodociągów wymaga bowiem kompleksowego podejścia. Takiego, które obejmuje zarówno inwestycje w nowoczesne technologie, jak i rozwój kompetencji pracowników. Wsparcie finansowe z Krajowego Planu Odbudowy (KPO), które umożliwi m.in. wdrożenie systemów IDS i SOC OT, pomoże znacząco zwiększyć odporność sektora na cyberzagrożenia. •

Inteligentny monitoring

ARTUR NOWAKOWSKI
Linc Polska



W procesie zarządzania tzw. smart city istotną rolę odgrywa technologia. Współczesne miasta to złożone organizmy. Obok czujników jakości powietrza oraz kontroli przepływu pojazdów to właśnie system monitoringu wizyjnego ma kluczowe znaczenie dla bezpieczeństwa mieszkańców. Obecność kamer w przestrzeni publicznej miast nie tylko odstrasza potencjalnych sprawców wykroczeń i przestępstw, ale także wspiera służby ratownicze i porządkowe w procesie reagowania oraz ustalania przyczyn i przebiegu zaistniałych incydentów.

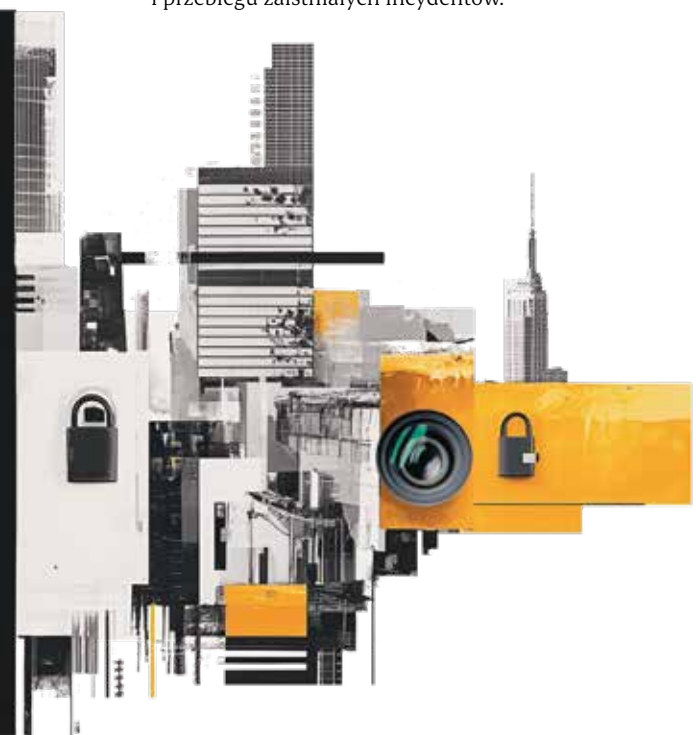
Kamery rozmieszczone w kluczowych miejscach, takich jak ulice, skrzyżowania, przystanki komunikacji miejskiej, place czy okolice szkół, umożliwiają bieżący nadzór i szybką interwencję w sytuacjach zagrożeń. W samej Warszawie znajduje się ponad 2 tys. kamer zintegrowanych z systemem zarządzania ruchem i transportem.

Skuteczne wykorzystanie systemu monitoringu wizyjnego zależy od wielu czynników. Jednym są umiejętności operatora, drugim możliwości ludzkiego umysłu. Percepcja człowieka jest ograniczona i może być zawodna. Eksperyment psychologiczny przeprowadzony przez Christophera Chabrisa i Daniela Simonsa (dotyczący tzw. niewidzialnego goryla) pokazuje, że przy skupieniu na konkretnym celu operator monitoringu może nie zauważyć niepokojących zdarzeń.

Wsparciem jest sztuczna inteligencja (AI), której możliwości ogranicza jedynie moc obliczeniowa. Analiza obiektowa pozwala wykrywać proste zdarzenia takie jak pojazdy jadące pod prąd czy zaparkowane w miejscu zakazanym. Ale dopiero dzięki wykorzystaniu AI możliwe staje się m.in. monitorowanie placu budowy w zakresie przestrzegania przez pracowników zasad BHP (np. weryfikacja, czy pracownicy noszą kamizelki i kaski) czy wykrywania osób, które się przewróciły. Są też dostępne bardziej złożone algorytmy, np. umożliwiające rozpoznawanie zachowań tłumu (gwałtowna ucieczka grupy z określonego miejsca). AI pozwala również na odnajdowanie w nagraniach wideo konkretnych wzorców poprzez wprowadzenie w wyszukiwarce prostego opisu np. „Znajdź człowieka w czerwonej kurtce z plecakiem”.

Powyższe narzędzia dają operatorowi możliwość bardziej efektywnego wykorzystania monitoringu miejskiego w celu automatycznej identyfikacji potencjalnych zagrożeń w przestrzeni publicznej.

Technologie rozwijają się bardzo dynamicznie. To co było nowością kilka lat temu, obecnie może już znacznie odbiegać od najnowszych implementacji AI. Dlatego warto stosować rozwiązania już sprawdzone, ale te, które na bieżąco dostosowywane są do najnowszych osiągnięć techniki. Ciągły i systematyczny rozwój systemów zabezpieczeń jest gwarancją ochrony przed aktualnymi zagrożeniami. •





Bezpieczeństwo przestrzeni publicznych

WOJCIECH KAWA

Ekspert ds. bezpieczeństwa



Generalnie można stwierdzić, że w Polsce zmniejszyło się zagrożenie w przestrzeni publicznej. Ma to związek z spadkiem przestępczości przeciwko mieniu. Malejące bezrobocie i wzrost gospodarczy, a także lepsza sytuacja finansowa gospodarstw domowych sprzyjają spadkowi przestępczości motywowanej ekonomicznie. Nic nie wskazuje na to, by ta tendencja miała się zmienić, ale policja musi na bieżąco analizować trendy w przestępczości, m.in. dotyczącej zorganizowanej przestępczości.

Najnowsze badania wskazują, że liczba wykroczeń i przestępstw koreluje z tym, jak zagospodarowana jest przestrzeń miejska. To tzw. teoria wybitych szyb. Głosi ona, że nawet drobne akty wandalizmu prowokują kolejne osoby do następnych, coraz bardziej szkodliwych i brutalnych zachowań. Konsekwencją jest zawłaszczanie części przestrzeni publicznej przez środowiska przestępcze. Polityka „zero tolerancji” zakłada brak akceptacji wobec nawet najdrobniejszych wykroczeń, takich jak wybita szyba czy spożywanie alkoholu w miejscach publicznych.

Bezpieczeństwo w przestrzeni publicznej zależy od wielu czynników, w tym od odpowiedniego planowania urbanistycznego, efektywnego monitoringu, skutecznego działania służb porządkowych i świadomości społecznej.

O tym, że przestrzeń publiczna jest bezpieczna, decyduje nie tylko brak zagrożeń (przestępczość, zachowania antyspołeczne), lecz także możliwość zaspokojenia potrzeb, zagwarantowanie warunków rozwoju, sprzyjanie budowaniu więzi społecznych. Krajowa Mapa Zagrożeń Bezpieczeństwa publikowana przez Komendę Główną Policji oraz dane dotyczące przestępczości pokazują, że to właśnie w ośrodkach miejskich notuje się największą liczbę incydentów.

Nowoczesne technologie wykorzystywane w budowaniu bezpiecznej przestrzeni

- 1. Centralne zarządzanie systemem bezpieczeństwa w mieście.** Taki system potrafi automatycznie wykrywać incydenty zagrożenia bezpieczeństwa (bójka, niszczenie mienia, picie alkoholu w miejscu publicznym, pozostawienie bagażu w newralgicznym punkcie itp.) i natychmiast wysyła alert do

odpowiednich służb, które są w stanie pojawić się na miejscu w ciągu kilku minut.

- 2. Wykorzystanie sztucznej inteligencji do bieżącej analizy obrazów z tysięcy kamer.** Kamery z inteligentnym oprogramowaniem umożliwiają identyfikację nietypowych zachowań, dokonują analizy twarzy i wskazują osoby poszukiwane, numery rejestracyjne pojazdów. Wykrywalność zagrożeń w przypadku tradycyjnego monitoringu ocenia się na 60%. Tymczasem system wykorzystujący technologię wideodetekcji zachowuje skuteczność na poziomie 95%.
- 3. Nowe wykorzystanie latarni miejskich.** Dotychczas służyły one do oświetlenia przestrzeni publicznej, dziś w jednej oprawie oświetleniowej można zainstalować wiele urządzeń: kamery monitoringu wizyjnego, czujniki jakości powietrza, kamery badające natężenie ruchu. Dzięki nim można usprawnić dojazd służb ratunkowych na miejsce wypadku. Niektóre miasta idą dalej, w San Diego jest testowana aplikacja, która dzięki czujnikom dźwięku ma pomóc identyfikować miejsca wystrzałów z broni palnej.
- 4. Wykorzystanie dronów.** Drony można wykorzystać do monitorowania obszarów, takich jak parki i place oraz poszukiwania osób zaginionych czy skadzionych pojazdów.
- 5. Inteligentne systemy zarządzania ruchem drogowym i pojazdami miejskimi.** Pomagają w zarządzaniu ruchem i reagowaniu na sytuacje awaryjne i kryzysowe. •

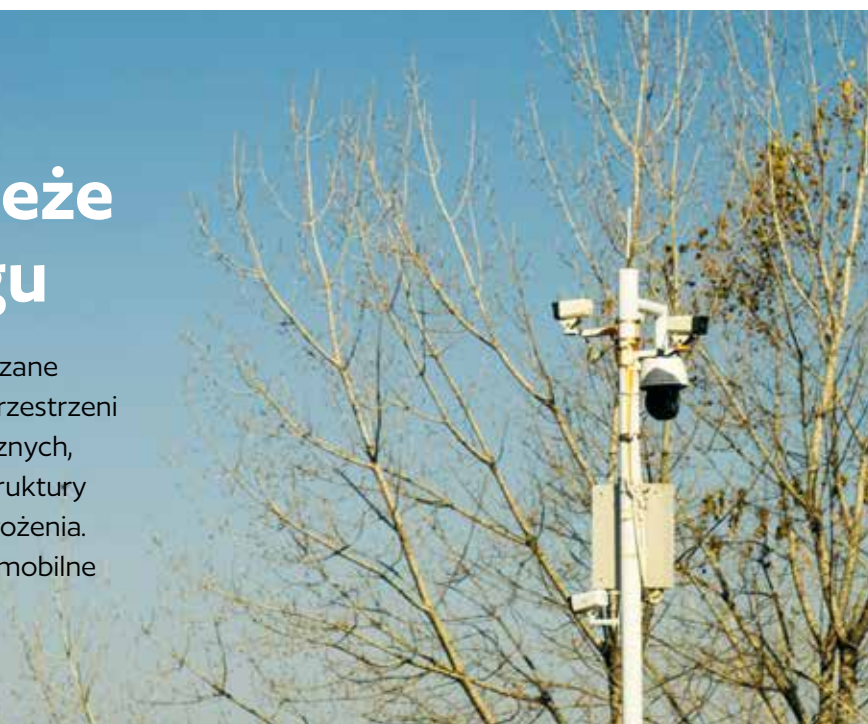




Mobilne wieże monitoringu

Współczesne wyzwania związane z ochroną osób, mienia czy przestrzeni wymagają rozwiązań elastycznych, niezależnych od stałej infrastruktury i gotowych do szybkiego wdrożenia. Na te potrzeby odpowiadają mobilne wieże monitorujące.

Krzysztof Bereza



Mobilne wieże oferują skuteczny dozór tam, gdzie stosowanie systemów stacjonarnie jest niemożliwe lub po prostu nieopłacalne. Ich popularność wzrosła zwłaszcza w sektorach budownictwa, energetyki odnawialnej, ochrony imprez masowych oraz zabezpieczeń infrastruktury krytycznej.

Wieże te najczęściej bazują na przyczepach z masztami teleskopowymi o wysokości od 4 do 10 m, co pozwala na montaż kamer obrotowych, termowizyjnych i stacjonarnych, oświetlenia LED, radarów oraz urządzeń komunikacyjnych. Mobilność rozwiązania pozwala na łatwe wdrożenie bez użycia ciężkiego sprzętu, a ich konstrukcja umożliwia relokację w ciągu kilkunastu minut, nawet przez jedną osobę.

Zasilanie mobilnych wież opiera się na kilku popularnych technologiach. Najczęściej stosowane są zestawy fotowoltaiczne połączone z akumulatorami AGM lub litowo-jonowymi, które zapewniają działanie przy odpowiednim nasłonecznieniu. W sytuacjach braku światła lub zwiększonego zapotrzebowania na energię systemy wspierane są przez generatory spalinowe lub rozwiązania hybrydowe, łączące różne źródła zasilania. Coraz bardziej popularne stają się alkoholowe ogniwa paliwowe, szczególnie metanolowe, które zapewniają cichą, niskoemisyjną i bezobsługową pracę przez wiele dni. Ogniwa te działają niezależnie od warunków atmosferycznych, emitując jedynie parę wodną i śladowe ilości dwutlenku węgla. Dzięki stabilnemu napięciu wyjściowemu oraz

kompaktowym rozmiarom coraz częściej są stosowane w miejscach, gdzie wymagana jest dyskrecja lub ciągłość działania przez długi czas bez obsługi.

Systemy detekcji montowane na wieżach wykorzystują zarówno analizę obrazu z kamer, jak i sygnały z czujek PIR, mikrofalowych oraz akustycznych. Coraz powszechniejsze są rozwiązania zintegrowane z algorytmami sztucznej inteligencji, które umożliwiają automatyczną klasyfikację obiektów, rozpoznawanie rejestracji pojazdów czy identyfikację nietypowych dźwięków. Radarowe detektory wykrywają ruch także w nocy oraz w warunkach ograniczonej widoczności. Atrakcyjnym rozwiązaniem są czujki zewnętrzne łączące się bezprzewodowo z wieżą. Umożliwia to ochronę rozleglejszych terenów o skomplikowanej topografii. Po wykryciu alarmu przez czujkę autonomiczną informacja o nim jest przesyłana do wieży, a zintegrowana kamera obrotowa kieruje się automatycznie w rejon wystąpienia alarmu, umożliwiając operatorowi weryfikację alarmu.

Transmisja danych jest realizowana za pośrednictwem sieci LTE/5G lub w przypadku bardziej zaawansowanych systemów – łączny radiowych i satelitarnych. Użytkownik może zarządzać systemem zdalnie, z poziomu aplikacji lub platformy VMS/PSIM. Ma przy tym pełen wgląd w obraz, historię alarmów oraz dostęp do danych archiwalnych.

Nowością na rynku są kompaktowe wieże mobilne, które stanowią odpowiedź na potrzeby krótkoterminowej i punktowej

ochrony. Urządzenia tego typu cechują niewielkie rozmiary, możliwość instalacji przez jedną osobę oraz pełna autonomia energetyczna dzięki wysokowydajnemu zasilaniu PV. Kompaktowe wieże są wyposażone w zestaw czterech czujników ruchu, które monitorują przestrzeń w zakresie 360 stopni. W razie wykrycia intruza czujnik wykonuje serię zdjęć i przesyła je do operatora. Natomiast wbudowana syrena alarmowa o wysokiej głośności i oświetlenie LED pełnią funkcję odstraszającą. Co ważne, aktywowane są automatycznie. Rozwiązanie to doskonale sprawdza się na mniejszych obszarach, takich jak kontenery, tymczasowe ogrodzenia, place montażowe czy niechronione odcinki robót drogowych.

Mobilne wieże monitorujące, zarówno klasyczne, jak i kompaktowe, znajdują szerokie zastosowanie w ochronie inwestycji drogowych, farm fotowoltaicznych i wiatrowych, wydarzeń plenerowych, terenów leśnych oraz obiektów strategicznych. Dzięki autonomii, niskim kosztom operacyjnym oraz integracji z nowoczesną analityką stanowią skuteczne i skalowalne narzędzie ochrony technicznej szczególnie tam, gdzie liczą się czas reakcji i dostępność, a przede wszystkim niezależność od stałej infrastruktury energetycznej i sieciowej. •

Polski Związek Pracodawców Ochrona

ul. Koszykowa 61, 00-667 Warszawa
<http://www.pzpochrona.pl>
biuro@pzpochrona.pl





LivEye – SMART BY DAY, SECURE BY NIGHT

W świecie, który w coraz większym stopniu jest kształtowany przez technologię, budownictwo stale się rozwija i otwierają się nowe możliwości. Innowacje, takie jak wirtualny portal LivEye, pokazują, w jaki sposób zaawansowane technologie mogą przekształcić i ulepszyć branżę.



Opcja Smart by Day rozszerza możliwości systemów LivEye i pozwala na ich podwójne zastosowanie: w ciągu dnia zapewniają wirtualny widok z placu budowy, a w nocy służą do ochrony obiektu. Dzięki temu LivEye oferuje korzyści przez całą dobę.

Budownictwo przez długi czas charakteryzowało się tradycyjnymi sposobami pracy opartymi na fizycznej obecności i procesach ręcznych. Jednak w ostatnich latach sytuacja uległa znacznej zmianie, ponieważ coraz więcej projektów budowlanych wykorzystuje innowacyjne technologie. Wirtualny widok placu budowy LivEye to dobitny przykład tego, że nawet tak analogowa branża, jak budownictwo, może zyskać lepszą wydajność dzięki digitalizacji niektórych procesów.

Czuje spojrzenie na plac budowy dzięki LivEye

Wieże monitorujące do dozoru wizyjnego są dziś niemal częścią standardowego wyposażenia placu budowy. Wykorzystanie ich podczas pracy na placu budowy w ciągu dnia jest tak samo ważne, jak w nocy i święta. Dzięki Smart by Day LivEye wieże oferują funkcję, która wykracza daleko poza konwencjonalne rozwiązania zabezpieczeń. Umożliwia ona wykorzystanie mobilnych systemów

monitoringu wizyjnego LivEye jako wirtualnego widoku placu budowy do monitorowania postępu prac i prowadzenia codziennego kalendarza. Kierownicy budowy i projektów mogą korzystać z przyjaznej dla użytkownika platformy internetowej, aby śledzić postępy budowy w czasie rzeczywistym, tworzyć filmy poklatkowe i oglądać plac budowy pod różnymi kątami.

Opcja Smart by Day firmy LivEye oferuje wiele korzyści dla projektów budowlanych:

• Dokumentacja i sprawozdawczość.

Wirtualny widok placu budowy pozwala na kompleksową dokumentację projektu, w tym zapisywanie filmów poklatkowych i archiwów obrazów. Szczególnie przydatne są obrazy 360° z pikselizacją w czasie rzeczywistym. Oprogramowanie oparte na sztucznej inteligencji łączy poszczególne obrazy z wież w panoramiczny widok do dokumentacji placu budowy, zamiast wykorzystywać je pojedynczo i statycznie. Oznacza to, że użytkownik może patrzeć we wszystkich kierunkach, a tym samym znacznie lepiej śledzić i dokumentować procesy budowlane.

• Zwiększona wydajność i mniejszy koszt inwestycji. Zdalne monitorowanie

postępów budowy pozwala na efektywniejsze planowanie i realizację projektów budowlanych. Możliwość pracy zdalnej pozwoli skutecznie zaoszczędzić na kosztach podróży.

• **Komunikacja i współpraca.** Zespoły projektowe mogą efektywnie komunikować się i współpracować z dowolnego miejsca za pośrednictwem platformy internetowej LivEye, co pomaga w utrzymaniu płynnego przebiegu projektu.

Przyszłość budownictwa z LivEye

Opcja Smart by Day firmy LivEye to pionierski przykład tego, jak technologia może zrewolucjonizować budownictwo. Dzięki integracji wirtualnych widoków placu budowy projekty budowlane mogą być bardziej wydajne, bezpieczniejsze i bardziej przejrzyste.

Podsumowując, nasze hasło *Secure by Night, Smart by Day* w prosty i elegancki sposób oddaje zalety naszych produktów: Indywidualne i elastyczne koncepcje bezpieczeństwa na noc, cyfrowe inteligentne rozwiązania na dzień. •



LivEye sp. z o.o.

ul. Ludwika Rydygiera 15/114
01-793 Warszawa
info@liveye.pl



Mobilne wieże do monitoringu BCS Mobilcam

BCS oferuje rozwiązania do monitoringu mobilnego w postaci przenośnych platform na podwoziu kołowym, ze składanymi masztami stanowiącymi podstawę do montażu zróżnicowanego typu urządzeń CCTV.

Dostępne są dwa typy podwozia – jeden z wieżą połączoną na stałe oraz drugi, w którym wieża i przyczepa stanowią oddzielne elementy. Dopuszczalna masa całkowita przyczepy zespolonej wynosi 750 kg, rozłącznej – 1200 kg. W drugim przypadku pozwala to na obsługę kilku wież za pomocą jednej przyczepy, która jest wyposażona w podnośnik hydrauliczny umożliwiający łatwy załadunek i rozładunek oraz w elementy zabezpieczające zapewniające bezpieczny transport ładunku. Samo rozstawienie wieży niezależnie od typu podwozia i przygotowanie do pracy nie powinno zająć jednej osobie więcej niż 30 min.

Najważniejszym elementem rozwiązania jest „skrzynia” zawierająca wszystkie podzespoły: 6-metrowy maszt wysuwany mechanicznie za pomocą wyciągarki ręcznej, obudowę z układami sterującymi oraz akumulatory podtrzymujące. Skrzynia pełni też funkcję zabezpieczającą przed dostępem nieupoważnionych osób.

Na szczycie masztu mogą zostać zamontowane dowolne urządzenia CCTV, jednak dla ułatwienia instalacji proponujemy klientom gotowe zestawy z produktami BCS Line lub BCS View. Najczęściej są to rejestrator oraz 4 kamery, co zapewnia obserwację wokół wieży w zakresie 360°. Jako wyposażenie dodatkowe zastosowano cztery promienniki IR. W obudowie umieszczono układ zasilania, switch łączący kamery z rejestratorem i router 5G zapewniający zdalny dostęp do systemu, a także termostat oraz grzałkę i wentylator, co pozwala na pracę w zmiennych

warunkach atmosferycznych. Znajduje się tu również moduł ładowania akumulatorów oraz dwa akumulatory 220 Ah, które zapewniają ciągłość pracy systemu w razie braku dostępu do zewnętrznych źródeł zasilania przez ok. 5 dni. Czas ten można wydłużyć, doposażając wieżę w rozkładane panele fotowoltaiczne. Nowością jest możliwość zastosowania agregatów prądotwórczych, pracujących na metanol. Stanowią one układ ładowania akumulatorów, a dzięki nim możliwe jest zapewnienie ciągłości pracy na okres ok. dwóch miesięcy. •

Więcej na: www.bcs.pl



Innowacyjna wieża monitorująca Janex International

Mobilna wieża monitorująca Janex International to innowacyjne rozwiązanie, które idealnie wpisuje się w rosnące potrzeby rynku. Wyposażona w zaawansowane technologie umożliwia monitorowanie różnorodnych miejsc, począwszy od placów budowy, przez parkingi, imprezy plenerowe, po tereny o dużej przestępczości czy farmy fotowoltaiczne.

Szeroki wybór opcji zasilania rozdzielnic teletechnicznych oraz zaawansowanych urządzeń monitorujących, takich jak kamery wysokiej rozdzielczości, sprawia, że wieża monitorująca dostosowuje się do indywidualnych potrzeb klientów, zapewniając im kompleksowe rozwiązanie w dziedzinie bezpieczeństwa.

Wieża mobilna jest zaprojektowana do zapewnienia niezawodnego zasilania w każdych warunkach. Pierwotnie jest zasilana z sieci elektrycznej, jednak w przypadku jej

awarii automatycznie przełącza się na alternatywne źródła energii, takie jak akumulatory, panele fotowoltaiczne, ogniwo paliwowe oraz agregat prądotwórczy PB/LPG.

Dla uzyskania maksymalnej mobilności wieża została zabudowana na przyczepce lekkiej, którą można transportować pojazdem, posiadając uprawnienia kat. B.

Wieża mobilna Janex International to innowacyjne rozwiązanie, które charakteryzuje się szeregiem unikalnych cech zapewniających jej wszechstronność, stabilność i funkcjonalność:

- wieża wolnostojąca lub zabudowana na przyczepce lekkiej o DMC do 750 kg,
- stabilna i bezpieczna konstrukcja stalowa,
- wysuwane cztery podpory w celu stabilizacji konstrukcji,
- drzwi z trzech stron umożliwiające pełny dostęp do wieży,
- zamykany dach,
- profesjonalny i mocny maszt

- podnoszony za pomocą ręcznej lub elektrycznej wyciągarki,
- wysokość wieży po wysunięciu masztu zabudowanego na przyczepce 6,5 m,
- uniwersalny stelaż na szczycie masztu przeznaczony do montażu urządzeń,
- rama montażowa dla trzech paneli fotowoltaicznych,
- zautomatyzowany agregat prądotwórczy PB/LPG.

Należy podkreślić, że Janex International jest polskim producentem, co dodatkowo potwierdza wysoką jakość i innowacyjność oferowanych produktów. Wieże są dostępne „od ręki”. •

Więcej na: www.janexint.com.pl





Securitas MobileCam – mobilna platforma monitoringu

Panele fotowoltaiczne lub agregat pozwalają urządzeniu działać do trzech tygodni na jednym zbiorniku paliwa, zapewniając funkcjonalność i prostą obsługę. Ma to kluczowe znaczenie w miejscach bez dostępu do stałego zasilania, takich jak infrastruktura krytyczna, tereny wyrębu, place budowy czy zgromadzenia publiczne. Samodzielność platformy w takich lokalizacjach wspiera łączność w technologii LTE.

Inteligentna analiza obrazu i termowizja

Zastosowanie kamer z inteligentną analizą obrazu w MobileCam pozwala skutecznie eliminować alarmy niestanowiące zagrożenia, np. wywołane przez ruch drzew, deszcz, śnieg czy obecność zwierząt. Termowizja zapewnia skuteczny monitoring w trudnych warunkach atmosferycznych,

np. przy zamgleniu lub słabym oświetleniu. MobileCam rejestruje obraz w wysokiej jakości w zakresie 360°, a wykrycie zagrożenia uruchamia alarm dźwiękowy i świetlny, widoczny dla intruza.

Securitas MobileCam

To efektywny, ekonomiczny, mobilny i w pełni wyposażony system ochrony:

- stosowany w trudnym terenie, bez stałego zasilania,
- maszt 6 m wyposażony w system kamer, oświetlacze światła białego i głośniki,
- autonomiczne zasilanie,
- inteligentna analiza obrazu i kamery



- termowizyjne zapewniające niezawodne wykrycie ruchu,
- ciągła rejestracja obrazu w 360° w wysokiej jakości,
- elastyczny czas wynajmu,
- podgląd i dostęp do nagrań online przez www i dowolne urządzenia. •

Więcej na: www.securitas.pl



Mobilna wieża monitorująca RTD od Uniforce

Mobilna wieża RTD firmy Uniforce została zaprojektowana z myślą o niezawodnym dozorcze terenu o ograniczonym lub całkowitym braku infrastruktury elektrycznej. To zaawansowane mobilne rozwiązanie umożliwiające szybkie wdrożenie monitoringu na placach budowy, farmach fotowoltaicznych, w mieście, na imprezach masowych i w innych środowiskach. Zapewnia niezależność energetyczną przez cały rok i może być indywidualnie konfigurowana pod potrzeby danego użytkownika.

Zalety:

- Niezależność energetyczna przez cały rok.
- Konkurencyjna cena.
- Wysoka odporność na wiatr i warunki atmosferyczne.
- Maszt wysuwany na wysokość 6,5 m.
- Zamykany dach chroniący wnętrze wieży.
- Przyczepa DMC 750 kg.
- Konfiguracja techniczna dostosowana do potrzeb użytkownika.
- Oszczędność w porównaniu z ochroną fizyczną.
- 3 panele fotowoltaiczne z regulacją kąta nachylenia.
- Automatyczne przełączanie źródeł zasilania (akumulatory, agregat, ogniwa paliwowe, 230 V).

Możliwości konfiguracji:

- Kamery PTZ, bullet, termowizyjne i rejestrator dowolnego producenta.
- Oświetlenie LED lub IR.
- Głośnik.
- Zaawansowana analityka obrazu.
- Systemy alarmowe i sygnalizacyjne.
- Moduły łączności GSM, radiowej lub satelitarnej.
- Turbina wiatrowa.
- Akumulatory.
- Agregat prądotwórczy na różne paliwa.
- Z przyczepą lub bez przyczepy.
- Dron ze stacją dokującą.



RTD to platforma, która łączy mobilność, odporność i swobodę konfiguracji. Projektowana pod konkretne wdrożenie, może być dostosowana do wymogów klienta – od rodzaju i liczby instalowanych urządzeń, po branding i integrację systemową.

Więcej na: www.uniforce.pl/wieza-rtd



iTower® Tripel Solar – zielona energia w praktyce!

Integracja alternatywnych źródeł energii stała się kluczowa do stworzenia mobilnego systemu dozoru wizyjnego, zdolnego do autonomicznej pracy. Połączenie paneli słonecznych i ogniw paliwowych EFOY marki SFC ENERGY w wieżach iTower® rozwiązało kwestię zasilania, oferując niezależny produkt przyjazny dla środowiska.

Można zapomnieć o czasochłonnym dostosowywaniu infrastruktury potrzebnej do uruchomienia wieży monitorującej i kilometrach kabli. Wieża iTower® Tripel Solar będzie działała skutecznie mimo braku dostępu do źródła prądu stałego, a do jej instalacji wystarczy tylko jedna osoba.

Wykorzystanie energii słonecznej i ogniw paliwowych EFOY

Trzy zintegrowane panele słoneczne pełnią funkcję głównego źródła zasilania, wykorzystując energię słoneczną, natomiast ogniwa paliwowe działają jako zapasowe

źródło energii, zapewniając nieprzerwaną pracę nawet w okresach niewielkiego nasłonecznienia lub złej pogody. Starannie zaprojektowana konstrukcja stelaża, w którym umieszczono panele, pozwala na ustawienie odpowiedniego kąta nachylenia, by zmaksymalizować ilość dostarczanej energii słonecznej.

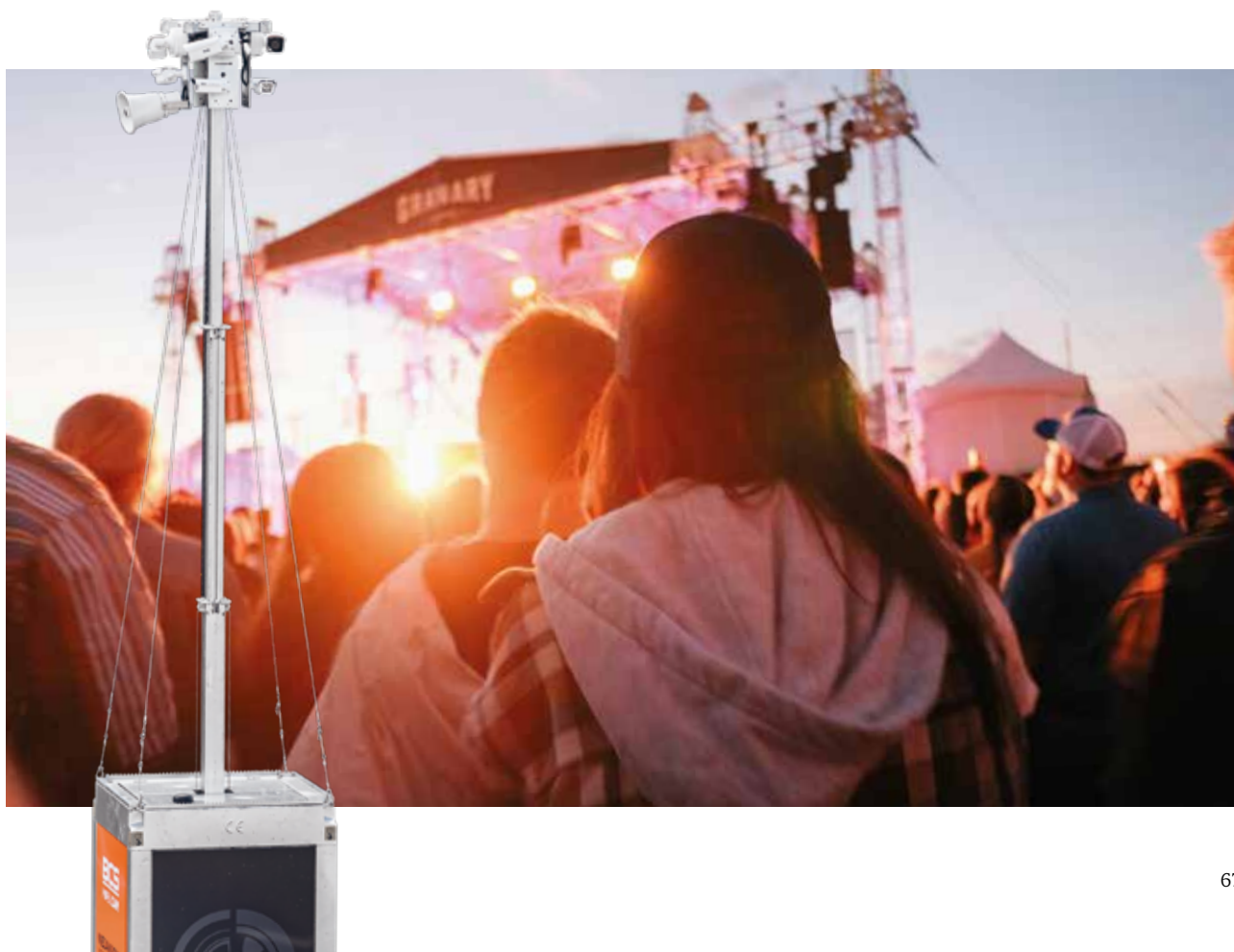
Możliwość podłączenia kilku kartridży z metanolem do jednego urządzenia EFOY sprawia, że nie trzeba martwić się o codzienne uzupełnianie paliwa. System może działać przez długi czas przy minimalnej interwencji człowieka. W przeciwieństwie do generatorów diesla jest przyjazny dla środowiska.

Rozwiązanie wykorzystywane na całym świecie

Nasi klienci, pochodzący z różnych zakątków świata, szczególnie doceniają jakość i profesjonalizm oferowanych przez nas rozwiązań. Jesteśmy wdzięczni, że obdarzyli nas zaufaniem. •



Więcej na www.vcs.pl

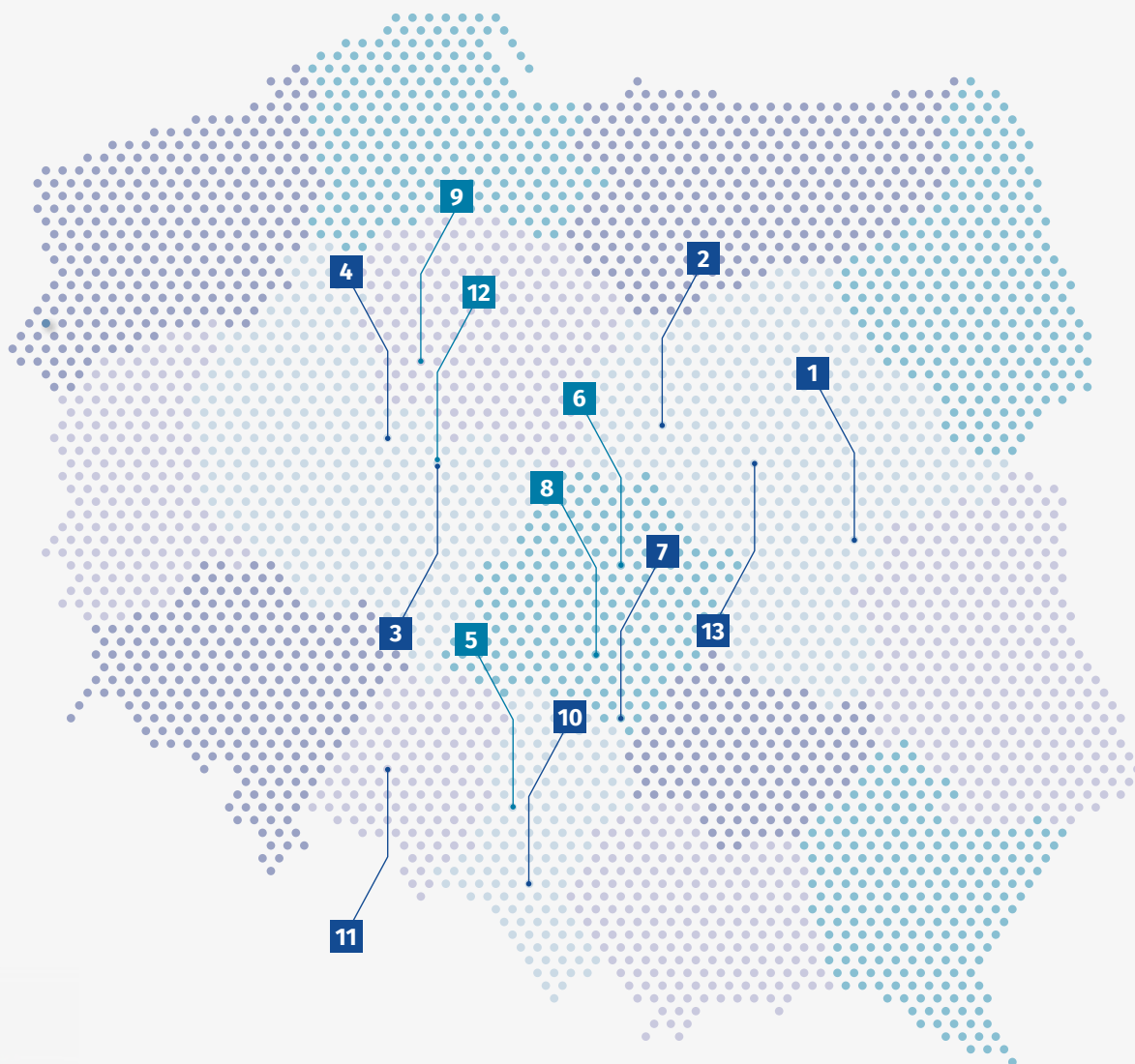




Mapa inwestycji

Na drugą połowę 2025 roku oraz kolejne lata planowane są liczne projekty infrastrukturalne i energetyczne realizowane przez czołowe polskie firmy budowlane. Inwestycje te obejmują zarówno modernizację istniejących obiektów, jak i budowę nowych jednostek, a ich lokalizacja rozciąga się na terenie niemal całego kraju – od Śląska, przez zachodnią i centralną Polskę. Wśród kluczowych przedsięwzięć znajdują się m.in. modernizacje stacji elektroenergetycznych, rozbudowa ciepłowni oraz budowa farm fotowoltaicznych i obiektów logistycznych. Projekty te nie tylko wspierają rozwój nowoczesnej infrastruktury energetycznej, ale także wzmacniają bezpieczeństwo energetyczne i efektywność transportu oraz przemysłu w Polsce.

Atrem	
1	Co: Modernizacje układów pomiarowo-rozliczeniowych JWCD oraz potrzeb ogólnych elektrowni Gdzie: Kozienice Kiedy: 30 miesięcy od dnia podpisania umowy (21.05.2025)
2	Co: Rozbudowa oraz modernizacja Systemu Ochrony Technicznej dla stacji NN Etap X (SE Płock) Gdzie: Płock Kiedy: 24 miesiące od dnia podpisania umowy (23.05.2025)
3	Co: Modernizacje układu elektroenergetycznego BWR3 w rejonie rozdzielnic OPR-R58a i OPR-R58b_ EPC Gdzie: Konin Kiedy: Kwiecień 2028 r.
4	Co: Budowa systemu ochrony kompleksu do obowiązujących przepisów i wymagań w kompleksie K-2725 Poznań CSWLąd Gdzie: Poznań Kiedy: 450 dni od dnia zawarcia umowy (12.05.2025)



Dekpol	
5	Co: Budowa parku logistycznego
	Gdzie: woj. śląskie
6	Kiedy: IV kwartał 2025 r. (zakończenie pierwszego z czterech etapów; trzy kolejne są opcjonalne)
	Co: Generalne wykonawstwo obiektu magazynowo produkcyjnego (centrum logistycznego)
6	Gdzie: k. Łodzi
	Kiedy: III kwartał 2026 r.

Elektrotim	
7	Co: Modernizacja kompleksowa stacji elektroenergetycznej 110/15 kV
	Gdzie: Dworzówce
	Kiedy: 24 miesiące od dnia zawarcia umowy (01.04.2025)

Energoaparatura	
8	Co: Wykonanie Głównego Punktu Odbioru, linii kablowej 110kV oraz rozdzielni 110kV GP22 w celu podłączenia farmy fotowoltaicznej 95MW „Pajęczno” wraz z jej uruchomieniem
	Gdzie: Pajęczno
9	Kiedy: 30.11.2026
	Co: Wykonanie części robót w ramach inwestycji polegającej na budowie Elektrowni Fotowoltaicznej Marulewy
9	Gdzie: Marulewy
	Kiedy: 22.12.2026

Mostostal Zabrze	
10	Co: Co: Rozbudowa istniejącej ciepłowni o blok parowy z kotłem wielopaliwowym
	Gdzie: Gliwice
	Kiedy: Koniec II kwartału 2028 r.
11	Co: Wielooperacyjny projekt modernizacji energetycznej Uniwersyteckiego Szpitala Klinicznego w Opolu
	Gdzie: Opole
	Kiedy: I kwartał 2028 r.

Prochem	
12	Co: Projekt przebudowy zakładu wytwarzania materiałów katodowych w Koninie
	Gdzie: Konin
	Kiedy: Październik 2025 r.

Unibep	
13	Co: Zaprojektowanie i wybudowanie hali utrzymaniowo-naprawczej pojazdów kolejowych
	Gdzie: Sochaczew
	Kiedy: 30 miesięcy od dnia podpisania umowy (15.04.2025)



Ster na bezpieczeństwo Bootcamp z widokiem na morze

Tegoroczna wiosenna edycja szkolenia strategiczno-terenowego Bootcamp odbyła się nad morzem, na malowniczej Wyspie Sobieszewskiej będącej dzielnicą Gdańska. Tym razem jako partnerów strategicznych zaprosiliśmy do współpracy firmy zajmujące się różnego rodzaju zabezpieczeniami: Axis Communications, CIAS Elettronica, Cube Solution, Genetec, Nedap, Securitas Polska oraz STid. Każda z nich

przygotowała dla uczestników zadania oparte na własnej technologii, aby można ją było sprawdzić w praktyce.

Pierwszy dzień upłynął na grze terenowej. Goście zostali podzieleni na sześć kiluosobowych grup, składających się z pracowników zbliżonych branż. Grupy kolejno odwiedzały stoiska partnerów rozlokowane na terenie hotelu oraz na samej plaży. Na stanowiskach uczestnicy

rozwiązywali zadania i przez kilkadziesiąt minut mogli na żywo testować poszczególne rozwiązania, zadawać pytania ekspertom, a także między sobą wymienić się wiedzą oraz know-how. Jak podkreślali wszyscy, to ten praktyczny wymiar spotkania zadecydował o jego profesjonalnym charakterze.

Wiele osób zwracało także uwagę na niezwykle pozytywną atmosferę panującą na Bootcampie. Po ponad sześciu godzinach spędzonych na testach i dyskusjach, a także wędrówkach między kolejnymi przystankami ogłoszono, która drużyna najlepiej poradziła sobie z zadaniami: Rekiny Ryzyka. Firmy wyróżniły także własnych faworytów, których nagrodziły drobnymi upominkami. Po wręczeniu nagród przyszedł czas na część nieformalną: kolację i ognisko.

Atrakcją drugiego dnia była wizyta referencyjna w terminalu kontenerowym Baltic Hub. Goście mieli okazję odwiedzić nie tylko trzy już operujące terminale, ale także dwa będące jeszcze w budowie, na żywo zobaczyć rozładunek kontenerowca, a także posłuchać o konstrukcji, funkcjonowaniu oraz zabezpieczeniach tego niezwykłego obiektu.

Bootcamp na Wyspie Sobieszewskiej okazał się dobrym połączeniem praktyki i wiedzy o najnowszych rozwiązaniach w branży security. •





Marek Skowronek,
Securitas

Po raz pierwszy Securitas wspólnie z Axis Communications prezentuje, jakie efekty może przynieść synergia działań, innowacji i technologii. Pokazujemy, jak tworzyć skuteczne systemy bezpieczeństwa – oczywiście wszystko oparte na sprzęcie najwyższej jakości.



Konrad Badowski,
Axis Communications

Pokazujemy nasze najnowsze rozwiązania technologiczne, na wspólnym stanowisku z naszym integratorem Securitas. Dzięki temu goście mogą dowiedzieć się, jakie technologie przygotowaliśmy, ale też jak są one wdrażane na rynku. Pokazujemy rozwiązania analityczne, w tym analizę obrazu opartą na głębokim uczeniu, sztuczną inteligencję.



Piotr Karpiński,
STid

Skupiliśmy się na NIS2 i ustawie o Krajowym Systemie Cyberbezpieczeństwa, która dotyczy też naszej branży, z czego jeszcze nie wszyscy zdają sobie sprawę. Dodatkowo pokazywaliśmy karty mobilne. Jest to rozwiązanie tańsze od kart fizycznych, bo płaci się za nie tylko raz.



Krzysztof Cichulski,
CIAS

Przygotowaliśmy dwie konkurencje. Jedna jest związana z czujkami zainstalowanymi na ogrodzeniu, które wykrywają próby przejścia. Zadaniem uczestników było dostawienie drabiny do płotu, a jeśli się udało bez wzbudzenia alarmu, to także próba wejścia chociaż na jeden stopień. Drugie zadanie polegało na uważnym słuchaniu tego, co mówimy o barierach mikrofalowych i ich martwych strefach.



Anna Twardowska,
Nedap Polska

Na 8. Bootcampie podeszliśmy w praktyczny sposób do normy dotyczącej kontroli dostępu EN60839. Zaczęliśmy od wprowadzenia, a potem daliśmy uczestnikom szansę na zastosowanie tej wiedzy. Przygotowaliśmy dla nich specjalne tablice, umożliwiające podejście do tego tematu w warsztatowy sposób.



Artur Koman,
Cube Solution

Na Bootcamp przygotowałem quiz wiedzy o bezpieczeństwie. Najpierw było to prawie 30 pytań o ochronę fizyczną, technologię, innowację, aż po AI, ale w trakcie ich zadawania okazało się, że większą wartość niż sama odpowiedź ma dyskusja, która wywija się w trakcie. Ostatecznie w quizie zostało 7 pytań, żeby wystarczyło czasu na wymianę doświadczeń.



Tomasz Nawrat,
Genetec

Przyjechaliśmy z naszym standardowym produktem, czyli Security Center. Dodatkowo pokazaliśmy Security Center SaaS, czyli rozwiązanie hybrydowe. Zaprezentowaliśmy możliwości dla klientów, którzy chcą przejść w chmurę, oraz możliwości, jakie mają ci, którzy chcą zostać z rozwiązaniem u siebie.

Damian Dziubałowski,
Komenda Stołeczna Policji



Bootcamp to dobra inicjatywa, ponieważ pozwala osobom, które zajmują się bezpieczeństwem obiektów czy przestrzeni publicznej, spojrzeć na kwestie bezpieczeństwa od innej strony. Takie podejście oferują obecni tu przedstawiciele firm, mający gotowe odpowiedzi na pytania, z którymi borykamy się nieraz miesiącami.

Mariusz Budny,
Kellanova



Mamy wspaniałą atmosferę i świetnych przewodników, którzy oprowadzają nas po stanowiskach. Mamy przekrój informacji, poczynwszy od obwodowej ochrony obiektu, przez kontrolę dostępu i kamery. Jest to ciekawe spotkanie i dobra okazja, żeby nawiązać kontakty z praktykami.



Karol Marcinkowski,
mBank



Na ósmym Security Bootcampie mieliśmy okazję odwiedzić sześć stanowisk z różnych obszarów bezpieczeństwa – od systemów kontroli dostępu, poprzez kamery, usługi ochrony. Jest to naprawdę superimpreza skierowana do wszystkich ludzi z branży, na której możemy wymienić się doświadczeniem z koleżankami i kolegami z różnych obszarów bezpieczeństwa.

Mateusz Stachowiak,
Bridgestone



Wymieniłem się wieloma doświadczeniami z ludźmi, którzy na co dzień pracują nad bezpieczeństwem. Rozmowy o sytuacjach, które oni mają u siebie w pracy, plus grono ekspertów, których mam tutaj do dyspozycji, na pewno ułatwią mi pracę. Ponadto z problemami, które mnie nurtują, mogłem tu uporać się w moment. Okazało się, że rozwiązania są na wyciągnięcie ręki.

Wojciech Styburski,
Agrointegracja



Reprezentuję środowisko agrobiznesu, integrujemy producentów rolnych. Jestem tu po to, żeby najnowszą technologię wspomaganą sztuczną inteligencją wprowadzić pod strzechy. Te technologie, które zostały tu zaprezentowane, pozwolą wdrożyć najnowsze systemy do zarządzania, np. stadem trzody chlewnej lub bydła.



Daniel Szyszko,
Baltic Hub



Drugi dzień Bootcampu to wizyta na największym w Polsce terminalu kontenerowym Baltic Hub. W związku z tym, że jesteśmy granicą państwa i obiektem portowym, zabezpieczenia są tu skomplikowane, a zastosowane rozwiązania bardzo ciekawe.



Public Safety Conference 2025: Granice, technologie, procedury. Jak wygląda bezpieczeństwo publiczne w Polsce?

Złożoność współczesnych zagrożeń bezpieczeństwa publicznego wymaga integracji działań służb, administracji i instytucji naukowych. Podczas Public Safety Conference 2025 eksperci z całego kraju omawiali aktualne wyzwania i dobre praktyki w zakresie ochrony granic, bezpieczeństwa wewnętrznego, wykorzystania nowoczesnych technologii oraz zarządzania kryzysowego.

Public Safety Conference 2025 to wspólne przedsięwzięcie firm Genetec (inicjatywa) i Sens Group (organizacja). Podczas jednodniowej konferencji w Warszawie w jednym miejscu spotkali się przedstawiciele resortów siłowych, urzędów miejskich, licznych instytucji państwowych, środowisk akademickich oraz firm oferujących rozwiązania i technologie dla sektora publicznego. Partnerami technologicznymi wydarzenia byli: Axis Communications, HID, Irisity, Hanwha Vision, Vivotek. Celem konferencji było stworzenie przestrzeni do rzeczowej i krytycznej refleksji nad realnym stanem bezpieczeństwa publicznego w Polsce – kraju położonym dziś na pierwszej linii geopolitycznego frontu.

Granica – linia obrony i przestrzeń testu

Część merytoryczną otworzył dr hab. Jarosław Truchan z Akademii Policyjnej w Szczecinie, przypominając o wyjątkowym położeniu Polski, na które składają się m.in. Przesmyk Suwalski czy nasza wschodnia granica, będąca jednocześnie wschodnią granicą Unii

Europejskiej. To położenie obecnie przysparza nam większej liczby zagrożeń niż szans. Chodzi rzecz jasna o sąsiedztwo z Białorusią – przez lata nieprzysparzające większych problemów, a od kilku lat będące nieustannie punktem zapalnym, w którym kumulują się wrogie zamiary wschodnich mocarstw względem Polski i, w dalszej kolejności, innych państw unijnych, krytyczna sytuacja życiowa podstępem zwerbowanych z pogranicza Azji i Afryki imigrantów, nieustępliwość polskich polityków i wytrwałość polskich służb.

– *Granica lądowa Polski jest najdłuższą granicą Unii Europejskiej zabezpieczaną przez pojedyncze państwo* – przypomniał prof. J. Truchan.

Dotychczasową ochronę zapewnianą przez cztery oddziały Straży Granicznej (warmińsko-mazurski, podlaski, nadbużański i beskidzki) wsparto siłami Wojsk Obrony Terytorialnej i Żandarmerii Wojskowej, a także szkoleniami Policji z Białegostoku. W obliczu

wojny w Ukrainie kluczowa okazała się blokada granicy. Prof. Truchan odmalował obraz alternatywny: gdyby jej zabrakło, służby musiałyby prowadzić długotrwałe akcje poszukiwawcze, co mogłoby osłabić ich zdolność do reagowania w lutym 2022 roku.

Nieocenioną rolę odegrały także nowe technologie – w tym zaporę elektroniczną złożoną z 500 słupów optoelektronicznych i czujników wykrywających fizyczne cechy obiektów.

Bezpieczeństwo wewnętrzne: między zaskoczeniem a procedurą

Ważnym punktem konferencji była debata poświęcona bezpieczeństwu w przestrzeni publicznej – zarówno tej miejskiej, jak i akademickiej. Punktem wyjścia stała się tragiczna śmierć portierki na Uniwersytecie Warszawskim, zamordowanej przez studenta w maju br.

Aneta Sadach z Uniwersytetu Łódzkiego zauważyła, że uniwersytety to instytucje z założenia otwarte. – *Bardzo trudno przewidzieć takie wydarzenia, zwłaszcza gdy sprawcą jest student. W tym przypadku zawiodło przekonanie, że skoro nigdy nic się nie stało, to nic się nie stanie* – powiedziała.

Ryszard Klimek dodał, że choć nie da się całkowicie wyeliminować zagrożeń, można ograniczyć ryzyko, np. przez wyposażenie pracowników „pierwszej linii kontaktu” w przyciski antynapadowe. Mariusz Galar da z Komendy Głównej Policji przypomniał,

Ryszard Kozłowski,
Urząd Miejski
w Łodzi



Możliwości Mission Control Genetec pozwolą na to, że korelacja zdarzeń będzie natychmiast wyświetlona na monitorach i umożliwi podjęcie konkretnych działań.

Aneta Sadach,
Wydział Filologiczny
Uniwersytetu Łódzkiego



Czułość, czujność i ograniczone zaufanie – to jest podstawa. Do tego technologia na pewno pomoże nam w lepszym zabezpieczeniu.

że choć każda instytucja ma inne procedury, to połączenie technologii i planowania może znacząco poprawić gotowość na niebezpieczne sytuacje.

Monitoring i sztuczna inteligencja: granice możliwości

Mariusz Czarnecki z Zakładu Obsługi Systemu Monitoringu m.st. Warszawy przybliżył działanie ZOSM – systemu tworzonego ponad dekadę temu, który dziś opiera się na ponad 600 kamerach, w tym mobilnych, oraz 170 operatorach zajmujących rotacyjnie 140 stanowisk. Użytkownikami systemu są różne instytucje miejskie, a zbierane dane mają kluczowe znaczenie dla podejmowania decyzji w czasie rzeczywistym.

Łukasz Olewiński z ZOSM zaznaczył, że choć rośnie liczba urządzeń, spada liczba ludzi je obsługujących. – *Nie korzystamy z AI. Naszą inteligencją są operatorzy – powiedział. – AI, zwłaszcza przy kamerach PTZ, nie poradzi sobie z błyskawiczną reakcją. Operatorzy natomiast tak. Od kilku lat notujemy sukcesy, jeśli chodzi o zapobieganie samobójczym skokom z mostów.*

Aneta Sadach również dostrzega potencjał w technologii: – *Korzystamy z technologii szeroko. Mamy zabezpieczenia zewnętrzne, szlabany z kamerami LPR. Wszystko to pomaga zarządzać infrastrukturą i uzyskiwać informacje o konkretnych wydarzeniach. Czynnikiem ludzki jest tym, który zawodzi najczęściej. System jest zimny – nie kieruje się emocjami, nie robi wyjątków.*

Nowe zagrożenia: żywność jako pole walki

Zaskakującym, ale ważnym wątkiem konferencji była kwestia bezpieczeństwa żywności. Jacek Tyburek przypomniał, że sabotaż żywności może być jednym z najtańszych i najskuteczniejszych sposobów ataku na społeczeństwo. Niestety tylko dwa miasta w Polsce – Warszawa i Wrocław – uwzględniają ten temat w planach zarządzania kryzysowego.



Przykład? Podczas niedawnej powodzi na Dolnym Śląsku pomoc żywnościowa była przechowywana i dystrybuowana w dużej mierze ad hoc. Część produktów – z powodu ryzyka skażenia – nie nadawała się do spożycia. Przypadek taki jak ten wpisuje się w zakres „Food Safety”, czyli tego wariantu ochrony przed nieintencjonalnym skażeniem. Ale zatrucie żywności może być także aktem jak najbardziej intencjonalnym (por. przypadek przedstawiony w serialu dokumentalnym „Wild Wild Country”: członkowie sekty zatrudnili się w barach sałatkowych w Oregonie i zakażali potrawy salmonellą). Możliwość sabotowania społeczności poprzez żywność jest co najmniej kilka, od biologicznego terroryzmu, przez terroryzm chemiczny, radiologiczny, po agroterroryzm.

Na stronie GIS, który jest punktem kontaktowym sieci RASFF po stronie polskiej, regularnie zamieszczane są ostrzeżenia przed zawartością m.in. bakterii, niebezpiecznych dla zdrowia związków chemicznych, a nawet cząsteczek plastiku w poszczególnych partiach żywności. Jak wskazał prelegent, Polska zajmuje niechlubne miejsce w czołówce

Monika Malczewska,
Urząd Miasta
Tomaszów Mazowiecki



W naszym mieście realizujemy dużo inwestycji, powstaje infrastruktura miejska, więc potrzeba coraz więcej kamer monitoringu, systemów, które będą zabezpieczać te miejsca i wpływać na bezpieczeństwo w mieście.

krajów, w których najczęściej dochodzi do tego typu nieprawidłowości.

Wnioski: bezpieczeństwo jako system naczyń połączonych

Public Safety Conference 2025 unaocniła, że współczesne bezpieczeństwo publiczne nie może być pojmowane w sposób wąski czy sektorowy. To system naczyń połączonych, obejmujący zarówno ochronę fizyczną granic, jak i reagowanie na kryzysy w przestrzeni miejskiej, gotowość uczelni do niespodziewanych incydentów i umiejętne wykorzystywanie technologii w służbie społecznej.

Eksperti byli zgodni co do jednego: skuteczność systemu bezpieczeństwa zależy od integracji zasobów – ludzkich, technologicznych i instytucjonalnych – oraz od zdolności do reagowania na zagrożenia, które nie są już tylko przyszłością, lecz rzeczywistością. Kluczowe pozostają inwestycje nie tylko w infrastrukturę, ale także w procedury, edukację i kulturę odpowiedzialności. •

Radosław Klimek,
Gdański Uniwersytet
Medyczny



Jeżeli chodzi o sztuczną inteligencję, to jej zastosowanie jest nieuniknione. Jeżeli będziemy mieli w systemie 800-900 kamer i 2-3 operatorów, oni nie będą w stanie wszystkiego zobaczyć.



CBC Poland

Usługi ochrony w czasach niepewności

Pod takim tytułem firmy CBC Poland i NEXT Software zorganizowały 29 maja br. konferencję dla firm ochrony. Partnerami wydarzenia były firmy EBS, Net-o-logy i Sekurak.pl. Gościem specjalnym był Santosh Munis, General Manager Działu Security CBC (Europe) w Londynie. W warszawskim hotelu Boss blisko 200 gości powitali Krzysztof Skowroński (CBC Poland) i Bartłomiej Dryja (Next Software).

To nie była zwykła konferencja produkto-
wa, choć nie zabrakło też pokazu najnowszych urządzeń. Wychodząc z założenia, że obecne zmiany geopolityczne powodują wzrost zagrożeń, gospodarze postawili na merytorykę.

W temat niepewności wprowadził uczestników dr Jacek Bartosiak, założyciel i właściciel

Strategy&Future. Naświetlił sytuację geopolityczną na świecie i zasugerował podjęcie natychmiastowych działań. W dzisiejszych czasach łatwy dostęp do informacji jest powodem rywalizacji, która będzie się pogłębiać. – *Wchodzimy w okres niepewności i chaosu. Warto się przygotować na niestabilne warunki funkcjonowania firm* – mówił J. Bartosiak.

Natomiast Piotr Caliński, AWCO, prawnik, ekspert ds. bezpieczeństwa biznesowego, podkreślił znaczenie analizy ryzyka. – *Biznes opiera się na informacjach i ich analizowaniu. To daje możliwość uniknięcia strat i uzyskania przewagi konkurencyjnej. Trzeba mieć więc strategię i pomysł na zbudowanie systemu ochrony* – radził P. Caliński.

Z kolei problemy bezpieczeństwa stacji monitorowania alarmów wyraźnie wskaza-
li Wojciech Górecki i Łukasz Płocke z portalu wizyjny.pl. – *Rozwiązaniem dla firm ochrony jest dziś inwestycja w nowoczesne narzędzia, w tym SI, oraz integracja systemów, a także dbanie o ich aktualizację. Brak aktualizacji to proszenie się o atak* – podkreślali prelegenci.

– *Bezpiecznie już było, a rolę security jest zbudowanie cyfrowej odporności* – stwierdził kolejny prelegent, Wojciech Muras z firmy Net-o-logy. W ubiegłym roku liczba incydentów związanych z cyberprzestępczością wzrosła o 30%. Koszty przestojów będących skutkiem ataków szacuje się na 10 mld dolarów.

Atak hakerski nie zawsze musi dotyczyć serwerów i komputerów. O tym, że hakować można kamerę CCTV, mówił Michał Sajdak z portalu Sekurak.pl, który podczas spotkania pokazał, jak takie ataki są przeprowadzane. Po jego wystąpieniu z pewnością wiele osób sprawdzało, czy wszystkie urządzenia monitoringu są na bieżąco aktualizowane i zabezpieczone.

Po części teoretycznej uczestnicy konferencji wzięli udział w warsztatach, podczas których mogli poznać najnowsze urządzenia GANZ Security oraz nowe funkcje Alice 1.5, czyli platformy AI do zarządzania stacjami monitoringu. •

Spotkanie Partnerów Handlowych Keenfinity (dawniej Bosch)

Na zaproszenie Keenfinity do olsztyńskiego hotelu przyjechało ponad sto osób. Spotkanie służyło przedstawieniu planów nowej odsłony firmy, kontynuującej część działalności w zakresie produktów technologii bezpieczeństwa i komunikacji Bosch Building Technologies.

O planach i perspektywach rozwoju opowiedział Michał Małek, dyrektor handlowy Keenfinity: – *To pierwsze spotkanie, podczas którego występujemy nie jako Bosch Building Technologies, ale Keenfinity sp. z o.o. Dzięki tej zmianie do Keenfinity przejdą trzy grupy produktowe: systemy wizyjne, systemy kontroli dostępu i alarmowe oraz*



systemy nagłośnienia i DSO, które przez kolejne lata będą jeszcze sygnowane marką Bosch. Jak zaznaczył Michał Małek: – *Mamy świadomość, że dokonanie udanego rebrandingu produktów zawsze wymaga czasu. W zależności od linii produktowej proces ten zajmie od dwóch do czterech lat. Oczywiście pracować będziemy też nad nowymi własnymi markami.*

– *Budujemy nową strategię produktową, ze sztuczną inteligencją przekształcającą tradycyjny monitoring w „inteligencję wizualną”.* Kamery już nie służą tylko do nagrywania, to wszechstronne narzędzia otwierające nowe możliwości w zakresie bezpieczeństwa i analizy danych – dodała Olga Zabłocka, specjalistka ds. marketingu.

Zmiana nie wpłynie na współpracę z partnerami. – *Spodziewamy się, że to będzie raczej ewolucja niż rewolucja. Oczywiście musimy zadbać o to, żeby nowe brandy były przez klientów rozpoznawane. Jednak wiemy, że dla naszych odbiorców liczą się przede wszystkim*

Keenfinity



jakość, bezpieczeństwo danych oraz strategiczne podejście do rozwoju produktu, z zachowaniem kompatybilności wstecznej. A to właśnie oferujemy – podkreślił M. Małek.

Jak wyjaśnił Marcin Grzybek, regionalny kierownik sprzedaży w dziale systemów kontroli dostępu i alarmów: – *Przekształcenie się w samodzielną firmę pozwoli nam rozwijać się dużo szybciej. Chcemy oferować nowoczesne i dobrze zabezpieczone produkty, z mobilnym dostępem z dowolnego miejsca. Bo to jest kierunek, w którym systemy zabezpieczeń podążają, szczególnie te dotyczące kontroli dostępu.*

Spotkaniu towarzyszyły także warsztaty, podczas których Keenfinity pokazało nowości oferowane w każdej z trzech grup produktowych. •

Integracja systemu kontroli dostępu RACS 5 z telewizją dozorową marki Hanwha Vision

Hanwha Vision działa na rynku elektronicznych zabezpieczeń od ponad 30 lat. Produkty CCTV tej marki cechuje wysoki poziom funkcjonalności, w zakresie gromadzenia i analizy danych, w tym analityki obrazu bazującej na AI.

Z kolei system kontroli dostępu RACS 5 jest przeznaczony do obiektów klasy biznes. Dzięki swojej szerokiej funkcjonalności zyskał on renomę sprawdzonego rozwiązania na rynku projektowym.

Obiekty, w których korzysta się z produktów i rozwiązań Hanwha Vision oraz systemu kontroli dostępu RACS 5, dobrze się uzupełniają. Integracja obu rozwiązań w naturalny sposób przynosi inwestorowi wymierne korzyści.

Integracja umożliwia:

- podgląd na żywo z kamer w oprogramowaniu do zarządzania systemem kontroli dostępu, monitorowanie na mapie obiektu pracy telewizji dozorowej z poziomu modułu SMS, jak i możliwość wyświetlania zdjęć lub wideo na żywo po wystąpieniu określonego zdarzenia – pozwala

to zbudować reguły zabezpieczeń automatyzujące obiekt, przekładające się na skuteczniejsze działanie ochrony;

- odtworzenie nagranego wideo dla konkretnych zdarzeń zarejestrowanych w systemie kontroli dostępu, gdy w systemie występuje rejestrator DVR/NVR – umożliwia to lepszą analizę zdarzeń niepożądanych i wskazanie osób za nie odpowiedzialnych;
- monitoring wizyjny systemu rejestracji i rozliczania czasu pracy – w ten sposób ogranicza się znacząco możliwość omijania zasad rejestracji czasu pracy w przedsiębiorstwie.

System RACS 5 jest zintegrowany z wieloma systemami CCTV. W sytuacji, gdy wymogiem

danego projektu jest zachowanie zgodności z ustawą NDAA, integracja RACS 5 z telewizją dozorową marki Hanwha Vision spełnia ten warunek. •



FLIR Scout Pro™ – monocular termowizyjny do zadań specjalnych

FLIR Scout Pro™ to najnowsza ręczna kamera termowizyjna marki Teledyne FLIR, którą charakteryzuje:

- szczegółowy obraz w zupełnej ciemności (<38 mK),
- szerokie pole widzenia (obiektyw o stałej ogniskowej z polem widzenia 32°),
- możliwość detekcji człowieka z odległości około 500 m,
- intuicyjność i łatwość obsługi nawet jedną ręką,
- kompaktowa, lekka obudowa,
- klasa szczelności IP67 oznaczająca pyłoszczelność i wytrzymałość na krótkotrwałe zanurzenie w wodzie,
- odporność na upadek z około 2 m,
- możliwość pracy do 6 godzin (bateria litowo-jonowa).

Ponadto monokular FLIR Scout Pro™ jest wyposażony w ekran o rozdzielczości XGA, który oferuje wyraźne odwzorowanie obrazu. Wbudowana pamięć 16 GB umożliwia rejestrację



zdjęć i nagrań wideo bezpośrednio w urządzeniu. Dodatkowa komunikacja bezprzewodowa może zapewnić transmisję obrazu na żywo do centrum nadzoru.

FLIR Scout Pro™ idealnie sprawdza się w działaniach organów ścigania, akcjach poszukiwawczo-ratowniczych oraz ważnych

operacjach zapewniających bezpieczeństwo publiczne.

W skrócie FLIR Scout Pro™ to połączenie komfortu obserwacji, wysokiej jakości obrazu z atrakcyjną ceną. •

www.linc.pl



Hakerzy nie odpuszczają

Czerwiec 2025 r. pokazuje, że cyberbezpieczeństwo to nie tylko globalne wyzwanie, lecz także lokalny priorytet. Rosnąca liczba ataków, wysokie koszty naruszeń i zwiększone budżety na ochronę zmuszają organizacje do inwestowania w nowoczesne rozwiązania oraz rozwój kompetencji, aby skutecznie reagować na dynamicznie zmieniający się krajobraz zagrożeń.

W I połowie 2025 r. liczba prób ataków ransomware może sięgnąć 289 mln, co oznacza, że aż 76,89% organizacji stanie w obliczu szantażu cyfrowego (raport *Top Cybersecurity Statistics & Trends for 2025*, opracowany przez VPNPrans). W tym samym raporcie wskazano, że ponad 1,08 mln osób może paść ofiarą phishingu, a unikalnych stron wyludżających dane może być ponad 1,6 mln. W dark webie krąży już ponad 1,7 mld skradzionych poświadczeń, co przyczyniło się do 42% wzrostu ataków opartych na przejęciu kont (*account takeover*), skutkujących m.in. kradzieżą pieniędzy albo co gorsza tożsamości.

Automatyczne skanowanie sieci osiągnęło 36 tys. na sekundę, czyli wzrost o 16,7% rok do roku, co ułatwia atakującym szybkie

wykrywanie luk w systemach, szczególnie w sektorze finansowym i e-commerce, o czym pisze TechRadar w artykule *AI Powering a Dramatic Surge in Cyberthreats*. To oznacza, że w każdej sekundzie na całym świecie dochodzi do 36 tys. pojedynczych prób połączenia się z różnymi adresami IP albo portami usług (np. SSH, HTTP, RDP). Innymi słowy, boty i skrypty w ułamku sekundy badają dziesiątki tysięcy miejsc w sieci. Z kolei prognozy mówią o ponad 3 tys. incydentach wycieków danych w 2025 r., a średni koszt pojedynczego naruszenia informacji opiewa na około 4,6 mln USD, uwzględniając koszty dochodzenia, powiadomień oraz rekompensaty strat klientów. Wzrost ten jest częściowo wynikiem zależności firm od infrastruktury chmurowej oraz zdalnej pracy, co otwiera nowe wektory ataku.

Wzrost wydatków na cyberbezpieczeństwo

Globalne budżety na cyberbezpieczeństwo mają wzrosnąć o 15,1% w 2025 r., osiągając 212 mld USD, co wynika z konieczności przeciwdziałania rosnącym zagrożeniom oraz

regulacjom prawnym (raport firmy badawczej Gartner *Wydatki na cyberbezpieczeństwo w 2025 roku wzrosną*). Oprogramowanie zabezpieczające, stanowiące ponad połowę rynku, rozwija się najdynamiczniej, z rocznym wzrostem 14,4%. Firmy inwestują w zaawansowane mechanizmy ochrony chmury, takie jak CNAPP (*Cloud Native Application Protection Platforms*), CASB (*Cloud Access Security Brokers*) i CWPP (*Cloud Workload Protection Platforms*).

Coraz częściej wdraża się systemy SIEM z modułami AI, które wykrywają anomalie w ruchu sieciowym w czasie rzeczywistym, co ma skrócić średni czas reakcji na incydenty (MTTR) nawet o 30%. Dodatkowo, rozwój narzędzi UEBA (*User and Entity Behavior Analytics*) pozwala na analizę nietypowych zachowań użytkowników i wczesne wykrywanie ataków wewnętrznych. W obliczu rosnących kosztów wycieków danych (4,6 mln USD za incydent), coraz więcej organizacji decyduje się na outsourcing usług SOC (*Security Operations Center*).

Sytuacja w Polsce

Według raportu „Barometr Cyberbezpieczeństwa 2025” autorstwa KPMG największym zagrożeniem w Polsce pozostają wycieki danych wywołane przez złośliwe oprogramowanie, wyprzedzające phishing oraz ataki DDoS, które zajęły trzecie miejsce pod względem częstotliwości. W pierwszych miesiącach 2025 r. odnotowano ponad 250 incydentów wycieków danych z polskich firm, generujących straty liczone w dziesiątkach milionów złotych. Eksperci wskazują, że przeciętny koszt naruszenia w Polsce wynosi około 3 mln USD, uwzględniając koszty prawne i operacyjne.

Wzrosło także zainteresowanie zabezpieczeniem łańcucha dostaw – 38% ankietowanych firm oceniło, że ryzyko ataków na podwykonawców znacząco się zwiększyło w porównaniu do 2024 r. Ataki tego typu mogą sparaliżować działalność kluczowych sektorów, takich jak energetyka czy finanse, dlatego coraz więcej organizacji przeprowadza audyty u dostawców oraz testy penetracyjne środowisk współpracujących.

Polski rynek nadal zmaga się z niedoborem wykwalifikowanych specjalistów – brakuje około 5 tys. ekspertów ds. bezpieczeństwa IT. Rośnie jednak liczba programów akademickich i bootcampów, które kształcą nowe talenty w zakresie etycznego hakowania, analizy zagrożeń oraz zarządzania incydentami. Inicjatywy te mają na celu zmniejszyć lukę kadrową i podnieść ogólny poziom świadomości w firmach, które coraz częściej inwestują w szkolenia swoich pracowników. •

check. create. manage.



Checly

the best startup 2023

checl.y.app

AcuSearch

Szukaj mądrzej, nie dłużej

AcuSearch umożliwia wyszukiwanie obiektu czy osoby na podstawie zaznaczonego fragmentu nagrania lub na podstawie cech fizycznych, koloru ubrania czy dodatków. To rewolucyjne rozwiązanie diametralnie skracające czas przeszukiwania nagrań umożliwiając, szybką interwencję.

