

RANKING SECURITY 50

Kto naprawdę wyznacza trendy na globalnym rynku security? Przedstawiamy zwycięzców i kierunki, które kształtują przyszłość branży.

**BEZPIECZEŃSTWO
W SKLEPACH**

Handel pod coraz większą presją. Jak chronić sklepy skutecznie i bez utraty komfortu klientów? Eksperti mówią wprost.

**BEZPIECZNE MUZEA –
JAK UNIKNĄĆ LOSU LUWRU**

Po kradzieży w Luwrze stało się jasne: odpowiednie zabezpieczenia i procedury to nie dodatek, a fundament działalności muzeów.



20 zł
(w tym 8% VAT)





Wesołych Świąt!

CIESZ SIĘ KAŻDYM INSPIRUJĄCYM MOMENTEM.

YEARS
salto 25



SALTO WECOSYSTEM
INSPIRED ACCESS



Salto Poland | saltosystems.com | +48 609 017 777



Przyszłość bezpieczeństwa dzieje się teraz

Organizacje mierzą się dziś z rosnącą liczbą zagrożeń – od cyberataków po wyzwania geopolityczne – dlatego skuteczna ochrona wymaga ciągłej modernizacji i współpracy między zespołami. Liczy się już nie tylko technologia, ale przede wszystkim jej odporność, adaptacyjność oraz kompetencje ludzi, którzy stoją za systemami. W najnowszym wydaniu pokazujemy, jak branża security reaguje na tę dynamikę i jakie kierunki wyznaczają liderzy rynku.

Rozpoczynamy relację z konferencji Warsaw Security Summit 2025 (str. 12), która jasno podkreśliła, że skuteczna ochrona to efekt połączenia technologii, kompetencji ludzi oraz dobrze zaprojektowanych procedur. Eksperti debatowali o narastających zagrożeniach hybrydowych, przyspieszonej transformacji cyfrowej oraz o tym, jak praktycznie wzmacniać cyberbezpieczeństwo w organizacjach. Coraz wyraźniej widać, że kultura bezpieczeństwa staje się fundamentem przewagi – buduje nie tylko skuteczność, ale także zaufanie.

Publikowane corocznie zestawienie Security 50 (str. 18) pokazuje, że globalna branża potrafi zachować odporność nawet w okresie silnych zawirowań gospodarczych. Firmy, które stawiają na innowacyjność i elastyczność, nie tylko utrzymują pozycję – potrafią ją umacniać. W Badaniu Trendów Technologicznych 2025 (str. 24) przyglądamy się temu, co naprawdę przynosi wartość. Indeks Dojrzałości i Przydatności Technologii odczarowuje marketingowe slogany i pozwala zobaczyć, które rozwiązania mają realne zastosowanie, a które wciąż szukają miejsca w praktycznych zastosowaniach.

W obszarze kontroli dostępu obserwujemy dynamiczną zmianę nawyków użytkowników. Mobilne przepustki i zamki bezprzewodowe stają się standardem wygody i elastyczności, a integracja w chmurze zmienia sposób zarządzania tożsamością i uprawnieniami.

Podobnie w sektorze monitoringu wizyjnego. Rok 2025 upłynął pod znakiem Edge AI – inteligencji przenoszonej jak najbliżej danych. Do tego silny trend kamer wieloprzetwornikowych, które pozwalają widzieć więcej, dokładniej i taniej. Potwierdzają to zarówno analizy rynkowe, jak i prognozy Memoori: automatyzacja, integracja i inteligencja będą fundamentami wzrostu. Swoje spojrzenie na transformację sektora przedstawiają także eksperci Omdia i Novaira Insights – ich wnioski pomagają lepiej zrozumieć przyszłość inwestycji w bezpieczeństwo.

Nie pomijamy handlu, gdzie wideoanalitika przestaje być narzędziem reakcji, a staje się narzędziem rozumienia. Dane z kamer ułatwiają projektowanie lepszych doświadczeń zakupowych oraz skuteczniejszą prewencję strat – dziś ma to znaczenie większe niż kiedykolwiek.

Najcenniejsze dobra narodowe wymagają ochrony adekwatnej do ich wartości, która wykracza daleko poza urządzenia i instalacje. Z wywiadu *Lekcja z Luwru: jak naprawdę powinny działać zabezpieczenia muzeów?* (str. 58) wynika, że skuteczna ochrona eksponatów zaczyna się długo przed instalacją kamer i czujek. Technologia jest tu narzędziem, nie celem: systemy zabezpieczeń muszą zostać zsynchronizowane z kompetencjami personelu, procedurami i architekturą samego muzeum. Jeśli choć jeden element zawiedzie, poczucie bezpieczeństwa okazuje się złudne.

To wydanie to przewodnik po najważniejszych trendach i decyzjach, które branża będzie podejmować dziś, aby jutro działać skuteczniej. Świat się zmienia – a my razem z nim. •

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

PRODUKTY NUMERU

- 8 Najnowsze urządzenia z oferty firm:**
BCS, Hikvision Poland, Linc Polska, Optex, TP-Link

WARSAW SECURITY SUMMIT

- 12 Warsaw Security Summit 2025 –**
bezpieczeństwo to proces, współpraca i kultura organizacyjna

SECURITY 50

- 18 Branża wykazuje odporność mimo silnych zawirowań gospodarczych**
William Pao
- 24 Badanie Trendów Technologicznych 2025: Indeks Dojrzałości i Przydatności Technologii**
asmag.com
- 26 Kontrola dostępu 2025: rosnąca popularność mobilnych przepustek i zamków bezprzewodowych**
William Pao
- 28 Monitoring wizyjny 2025: Edge AI i kamery wielosensorowe na czele**
William Pao
- 30 Nowe kierunki rozwoju rynku kontroli dostępu**
Prasanth Aby Thomas
- 34 Co kształtuje rynek monitoringu wizyjnego**
Prasanth Aby Thomas
- 38 Siedem kluczowych trendów kształtujących rynek monitoringu wizyjnego**
Owen Kell, Memoori Research
- 40 Rewolucja AI w security: między innowacją, inteligencją a regulacjami**
Tommy Zhu, Omdia
- 42 Novaira Insights analizuje globalny rynek monitoringu wizyjnego**
asmag.com

REDAKCJA

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

PREZES ZARZĄDU
Mariusz Kucharski

REDAKTOR NACZELNA
Marta Dynakowska

Z-CA RED. NACZELNEGO
Jan T. Grusznic

REDAKCJA
Monika Żuber-Mamak
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
Jan Kurzawa

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

Czujność

KAMERY DWUPRZETWORNIKOWE

TERMICZNA + WIZYJNA

BCS-L-TIP541FSR3-FDT(0401)

BCS-L-EIP541FSR2-FDT(0401)

Technologia radiometryczna • Przeznaczona do detekcji ognia i pożaru

Rekomendowany zasięg detekcji 10m • Obiektyw termiczny 1.2mm

Pomiar temperatury -10°C~+200°C max (±5°C, ±5%)

Kamera wizyjna 4Mpx z przetwornikiem 1/2.7" i obiektywem 4mm • Promiennik podczerwieni 30m

Wbudowany mikrofon, głośnik • Alarmy dźwiękowe i świetlne

>> Więcej przeczytasz na stronie 8



www.bcs.pl
www.facebook.com/bcspl
www.instagram.com/bcskamery



Spis treści

HANDEL

- 44 Jak wideoanalitka pomaga zrozumieć zachowania kupujących w sklepach**
Hikvision Poland
- 46 Rosnące straty w handlu – problem, który wymaga reakcji**
Checkpoint Systems
- 48 Głos branży**

RYNEK SECURITY

- 54 Lekcja z Luwru: jak naprawdę powinny działać zabezpieczenia muzeów?**
Wywiad z Arturem Boguszem, kierownikiem działu bezpieczeństwa Muzeum Historii Polski
- 56 Bezpieczne muzea**
Monika Brodawska, PZPO
- 57 Zintegrowane bezpieczeństwo w nowej fabryce Ernst & Engbring. Kompleksowa realizacja C&C Partners**
C&C Partners
- 58 Ogólnie acz szczegółowo – kamery MSC**
Jan T. Grusznik
- 62 Przegląd kamer panoramicznych z oferty firm:**
BCS, CBC Poland, CCTV Baltic, Urkom, Vivotek
- 65 Bezpieczeństwo jutra: przyszłość ochrony fizycznej**
Wywiad z Markiem Skowronkiem, członkiem Zarządu w Securitas Polska

CYBERBEZPIECZEŃSTWO

- 66 Strategiczne podejście do projektów bezpieczeństwa**
Daniel Kamiński

SERWIS INFORMACYJNY

- 68 Milestone Technology Day Poland 2025:**
technologia, która rozumie świat
- 70 Nowości rynkowe**





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.



Prezentujemy najnowsze urządzenia z oferty firm

BCS, HIKVISION, LINC POLSKA, OPTEX, TP-LINK



BCS

Skuteczne wykrywanie zagrożeń pożarowych

Kamera BCS-L-EIP541FSR2-FDT i jej odpowiednik w obudowie tubowej BCS-L-TIP541FSR3-FDT to nowoczesne urządzenia bispektralne, które łączy funkcje kamery termowizyjnej i klasycznej kamery wizyjnej. Dzięki temu zapew-

nia kompleksowe monitorowanie przestrzeni oraz skuteczne wykrywanie zagrożeń pożarowych.

Zastosowany w niej niechłodzony detektor VOx o rozdzielczości 120×90 pikseli pozwala na precyzyjne obrazowanie w podczerwieni, a czułość poniżej 60 mK umożliwia szybkie wychwycenie nawet niewielkich różnic temperatur. Kamera jest w stanie wykrywać płomienie o wymiarach 10×10 cm z odległości do 10 metrów, a także mierzyć temperaturę w zakresie od -10 do 200°C z dokładnością ±5°C. To czyni ją szczególnie przydatną w garażach podziemnych, halach przemysłowych czy magazynach, gdzie ryzyko pożaru jest wysokie.

Oprócz modułu termowizyjnego kamera ma przetwornik CMOS o rozdzielczości 4 Mpix. Dzięki obiektywowi o ogniskowej 4 mm oraz wysokiej czułości przy słabym oświetleniu możliwe jest uzyskanie wyraźnego obrazu nawet w trudnych warunkach. Wbudowany oświetlacz IR LED o zasięgu do 15 m dodatkowo wspiera pracę w całkowitej ciemności. Kamera obsługuje kompresję H.265, H.264 oraz MJPEG, co pozwala na efektywne zarządzanie pasmem i przestrzenią dyskową.

BCS-L-EIP541FSR2-FDT to rozwiązanie przeznaczone do obiektów, w których kluczowe znaczenie ma szybkie wykrycie pożaru i możliwość wizualnej weryfikacji zagrożenia. Dzięki połączeniu obrazu termicznego i wizyjnego kamera nie tylko zwiększa skuteczność detekcji, ale także wspiera działania prewencyjne i ratownicze, stanowiąc istotny element nowoczesnych systemów bezpieczeństwa. •

Więcej na: www.bcs.pl



HIKVISION

Hikvision DS-K270X i DS-K262X – bezpieczne zarządzanie dostępem

Seria kontrolerów dostępu Hikvision DS-K270X i DS-K262X to nowoczesne rozwiązania stworzone z myślą o bezpiecznym, skalowalnym zarządzaniu dostępem w firmach, instytucjach i obiektach publicznych.

Kontrolery DS-K270X integrują wysoką wydajność z prostotą konfiguracji, umożliwiając obsługę wielu punktów wejścia oraz elastyczne dopasowanie do istniejącej infrastruktury. Modele wyróżniają się szybkim przetwarzaniem danych oraz obsługą dużej liczby użytkowników, co sprawdza się w miejscach o intensywnym ruchu.

Seria DS-K262X oferuje rozszerzone możliwości integracji z systemami monitoringu i alarmowymi Hikvision, zapewniając centralne zarządzanie bezpieczeństwem. Obie linie wspierają zaawansowane funkcje, takie jak autoryzacja kartą, PIN-em czy harmonogramy dostępu. Solidna konstrukcja i stabilna praca czynią je niezawodnymi elementami profesjonalnych systemów kontroli dostępu. •

Więcej na: www.hikvision.com/pl/



RACS 5



ASSA ABLOY

Nowoczesna transformacja bez rewolucji

Nowy system, ta sama instalacja.

Wykorzystaj istniejącą infrastrukturę i zyskaj nowe możliwości.

Maksymalne bezpieczeństwo. Minimalny wysiłek.

Protokół OSDP, szyfrowana komunikacja, Grade 4 – najwyższy poziom w standardzie.

Nowoczesność w praktyce: efektywność, komfort, elastyczność.

Wydajna baza SQL, bezpieczna identyfikacja mobilna i wielostanowiskowa architektura.

Jeden system. Pełna kontrola.

Zarządzaj dostępem, monitoruj i wizualizuj zintegrowane systemy bezpieczeństwa – wszystko z jednego miejsca.

Technologia, która myśli jak Ty.

Nowoczesny interfejs, intuicyjna obsługa, pełna kontrola.

Zainwestuj w przyszłość – dziś.

RACS 5 to długoterminowe wsparcie i rozwój.



Experience a safer
and more open world



LINC POLSKA

FLIR Scout Pro™ do zadań specjalnych



FLIR Scout Pro™ to monokular termowizyjny marki Teledyne FLIR zaprojektowany z myślą o pracy w wymagających warunkach terenowych. Dzięki czułości poniżej 38 mK kamera oferuje szczegółowy obraz w zupełnej ciemności, co pozwala na skuteczne wykrywanie obiektów nawet przy minimalnych różnicach temperatur. W FLIR Scout Pro™ zastosowano obiektyw o stałej ogniskowej z szerokim polem widzenia 32°, który umożliwia detekcję sylwetki człowieka z odległości około 500 metrów.

Scout Pro™ wyróżnia się prostotą obsługi – z urządzenia można wygodnie korzystać jedną ręką, co ma znaczenie w dynamicznych działaniach terenowych. Kompaktowa, lekka konstrukcja o klasie szczelności IP67 gwarantuje odporność na pył, deszcz oraz krótkotrwałe zanurzenie w wodzie, a także zabezpiecza kamerę przed skutkami upadku z wysokości ok. 2 m. Wbudowana bateria litowo-jonowa umożliwia nieprzerwaną pracę nawet do 6 godzin.

Monokular wyposażony jest w ekran o rozdzielczości XGA zapewniający wyraźne odwzorowanie szczegółów. Wbudowana pamięć wewnętrzna 16 GB pozwala na zapis zdjęć i nagrań bezpośrednio w urządzeniu, a opcjonalna komunikacja bezprzewodowa umożliwia transmisję obrazu na żywo do centrum dowodzenia. FLIR Scout Pro™ doskonale sprawdza się w działaniach służb mundurowych i organów ścigania oraz operacjach poszukiwawczo-ratowniczych. Monokular FLIR to praktyczne narzędzie dla profesjonalistów, które łączy wysoką jakość obrazu i wygodę użytkowania z atrakcyjną ceną. •

Więcej na: www.linc.pl

OPTEX

REDSKAN Lite – nowy model w serii czujek LiDAR

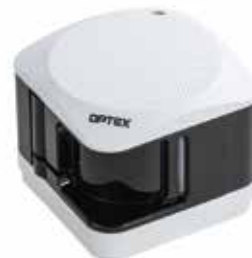
OPTEX, światowy lider w dziedzinie detekcji, prezentuje nowy model z wielokrotnie nagradzanej serii czujek LiDAR. REDSCAN Lite RLS-1010L to kompaktowe urządzenie zaprojektowane z myślą o ultraszybkiej i wyjątkowo precyzyjnej detekcji krótkiego zasięgu w środowiskach wewnętrznych, w których wymagany jest najwyższy poziom bezpieczeństwa.

REDSKAN Lite oferuje skuteczną ochronę wąskich lub trudno dostępnych przestrzeni. Dzięki zaawansowanej technologii *Time of Flight* czujka jest w stanie zidentyfikować obecność intruza w obszarze o wymiarach 10 x 10 metrów w czasie zaledwie 100 milisekund. REDSCAN Lite zapewnia niezawodne działanie niezależnie od warunków oświetleniowych i zmian temperatury. Detekcja jest możliwa także w całkowitej ciemności.

Czujka REDSCAN Lite może być instalowana w pozycji zarówno poziomej, jak i pionowej, w zależności od wymagań aplikacji. W pozycji poziomej tworzy niewidzialną płaszczyznę detekcji, która doskonale sprawdza się przy zabezpieczaniu przestrzeni pod sufitami oraz świetlikami. W pionowej konfiguracji umożliwia skuteczną ochronę cennych aktywów, szaf rack, wąskich przejść oraz stref o ograniczonym dostępie.

Zastosowanie wysokiej rozdzielczości oraz błyskawicznego czasu reakcji pozwala na natychmiastowe wykrycie każdego naruszenia ściśle zdefiniowanej strefy. Detekcja odbywa się wyłącznie w precyzyjnie wyznaczonym obszarze, co pozwala wyeliminować ryzyko fałszywych alarmów i zapewnić skuteczną ochronę tam, gdzie tradycyjne technologie mogą okazać się niewystarczające. •

Więcej na: www.optex-europe.com/pl



TP-LINK

Kamery TP-Link VIGI InSight – pełny obraz bezpieczeństwa

TP-Link prezentuje nową serię kamer VIGI InSight, stworzoną dla firm i instytucji, które potrzebują niezawodnego monitoringu o wysokiej jakości – zarówno w dzień, jak i w nocy. Urządzenia łączą zaawansowaną technologię obrazu z intuicyjną obsługą, umożliwiając szybkie budowanie skalowalnych systemów nadzoru.

Dzięki nowej generacji przetworników, technologii ColorPro 2.0 oraz inteligentnym funkcjom analitycznym kamery rejestrują każdy detal z wyjątkową precyzją,



niezależnie od warunków oświetleniowych czy pogodowych.

VIGI InSight S345S to zewnętrzna kamera 4 Mpix typu bullet wyposażona w jasną przysłonę F1.0 i przetwornik 1/1,79", które zapewniają realistyczny kolorowy obraz nawet po zmroku. Moduł AS-ISP automatycznie redukuje szumy i rozmycia, a zaawansowana detekcja oraz klasyfikacja ludzi i pojazdów znacząco ograniczają liczbę

fałszywych alarmów. Kamera oferuje dodatkowo dwukierunkową komunikację, alarm świetlny-dźwiękowy oraz port Alarm In/Out, pozwalający na integrację z zewnętrznymi systemami, np. syreną lub ochroną obiektu.

VIGI InSight S445S oferuje identyczne możliwości technologiczne w kompaktowej obudowie Turret, idealnej do miejsc wymagających dyskretnego, ale skutecznego monitoringu.

Seria VIGI InSight została zaprojektowana z myślą o małych i średnich firmach oraz instytucjach publicznych – od parkingów i terenów zewnętrznych po obiekty rekreacyjne. Zarządzanie wszystkimi urządzeniami jest proste dzięki aplikacji mobilnej i oprogramowaniu VIGI. Kamery objęte są 3-letnią gwarancją producenta. •

Więcej na: www.tp-link.com/pl/



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



OFICJALNY DYSTRYBUTOR:

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



WWW.LINC.PL

Linc
Polska Sp. z o.o.



– bezpieczeństwo to proces, współpraca i kultura organizacyjna

Za nami kolejna, intensywna i niezwykle inspirująca edycja **Warsaw Security Summit 2025**. Wydarzenie ponownie potwierdziło, jak szybko ewoluuje krajobraz zagrożeń oraz jak kluczowa staje się współpraca między biznesem, administracją publiczną i branżą technologiczną w budowaniu odpornego i nowoczesnego ekosystemu bezpieczeństwa.





W trakcie dyskusji i prelekcji eksperckich dominowały tematy związane z transformacją cyfrową, rozwojem zagrożeń hybrydowych oraz praktycznymi aspektami współczesnego cyberbezpieczeństwa. Uczestnicy i prelegenci zgodnie wskazywali na kilka kluczowych kierunków rozwoju:

- **dynamiczny wzrost znaczenia sztucznej inteligencji** w detekcji i zapobieganiu incydentom;
- konieczność budowania odporności organizacyjnej poprzez procesy, procedury i edukację, wykraczającą poza samą technologię;
- **wartość dzielenia się wiedzą i doświadczeniami** między instytucjami i sektorami;
- **świadomość, że bezpieczeństwo to nie jednorazowy projekt**, lecz ciągły proces i element kultury organizacyjnej.

Serdecznie dziękujemy wszystkim prelegentom za ekspercką wiedzę, profesjonalizm oraz inspirujące wystąpienia. Wyrazy uznania kierujemy także do naszych partnerów, bez których realizacja wydarzenia nie byłaby możliwa:

Axis Communications, CCTV Baltic Sp. z o.o., Elmark Automatyka S.A., HID, Megavision Technology Sp. z o.o., Milestone Systems, IBM, squareTec, Rządowe Centrum Bezpieczeństwa, Uniwersytet Civitas.

Dziękujemy wszystkim uczestnikom za obecność, cenne rozmowy i współtworzenie przestrzeni wymiany kompetencji i nowych perspektyw.

**Mariusz Kucharski,
a&s Polska**

– To już dziewiąta edycja konferencji Warsaw Security Summit, na której gromadzimy liderów bezpieczeństwa. W programie wystąpienia wybitnych ekspertów, ludzi, którzy mówią nie tylko o teorii, ale także o praktyce, o swoich doświadczeniach.





**Gen. Mieczysław Bieniek,
doradca MON, były zastępca dowódcy strategicznego NATO**

– Zmieniło się dużo. Dynamika zmian jest olbrzymia i cieszy mnie to, że dziewiąta edycja Warsaw Security Summit podjęła te tematy. Zmieniła się również świadomość społeczna postrzegania zagrożeń. W zakresie sił zbrojnych zdynamizowaliśmy proces organizacji tychże sił, ich wyposażenia, świadomości szkolenia i zaangażowania sojuszników w systemy obronne.

Mjr dr Anna Grabowska-Siwiec, oficer kontrwywiadu ABW w latach 2004-2020

– Tak do końca nie wiemy, skąd przyjdzie zagrożenie. Państwo nie reaguje wystarczająco dynamicznie na zagrożenia, które w tej chwili powstają ze strony obcych wywiadów. Pracownicy, czy instytucji państwowych, czy instytucji prywatnych, powinni być objęci większą ochroną, częstszymi szkoleniami, budowaniem świadomości, pokazywaniem, co można zrobić w określonych sytuacjach albo czego nie robić.



Jerzy Smoliński, Uniwersytet Civitas

– Człowiek, człowiek, człowiek. Od tego powinniśmy zacząć. I na człowieku powinniśmy skończyć. To zawsze było i jest najsłabsze ogniwo, jeśli chodzi o działania związane z bezpieczeństwem. I szkoleniu tego człowieka trzeba poświęcić dzisiaj więcej czasu. Bo ten człowiek został na pewnym etapie szkolenia, a technologia, która jest dostępna w nowoczesnych firmach, jest po prostu na dużo wyższym poziomie. I ta przepaść musi zostać wypełniona za pomocą szkoleń, także takich konferencji jak tu dzisiaj.

Andrzej Mroczek, Uniwersytet Civitas

– Z punktu widzenia osoby odpowiedzialnej za bezpieczeństwo jest istotne, jak przygotować się na potencjalne zagrożenia, czyli przede wszystkim zrobić analizę ryzyka, tak aby w sposób proaktywny podejść i właściwie reagować na tego typu niebezpieczeństwa.



**Dorota Duda,
Rządowe Centrum Bezpieczeństwa**

– Bardzo ważne jest budowanie kultury bezpieczeństwa w każdej organizacji w myśl cyklu Deminga: zaplanuj, zrób, monitoruj, ale wyciągaj też wnioski, czyli doskonał.



**Bogumił Szymanek,
Axis Communications**

– Podczas tego wydarzenia uczestnicy mogli posłuchać naszego eksperta ze Szwecji, który omawiał tematykę przetwarzania obrazu i jego modyfikacji w czasach sztucznej inteligencji. Dodatkowo uczestnicy mogli brać udział w warsztatach poświęconych technologii radarowej prowadzonej przez Jarka Sapko.



**Kamil Barański,
Megavision Technology**

– Myślę, że w najbliższym roku wszyscy spotkamy się w nowej rzeczywistości, gdzie będziemy rozmawiać o szerokim wykorzystaniu sztucznej inteligencji. Musimy efektywnie przyglądać się temu, w jaki sposób sztuczna inteligencja będzie w stanie pomóc nam w zarządzaniu biznesem.



**Jan T. Grusznic, squareTec**

– Najważniejszym elementem przy zastosowaniu sztucznej inteligencji jest jej świadome wykorzystanie w bezpieczeństwie. To wiedza na temat samych detekcji, używania narzędzi, ale też związana bezpośrednio z zarządzaniem, odpowiedzią na wskazanie incydenty.

**Piotr Benke, CTO IBM Polska**

– Generatywna sztuczna inteligencja zarówno wprowadziła wiele podatności do systemów, w których jest wykorzystywana, jak i sama staje się źródłem nowych, dotąd nieznanych zagrożeń. Przykładem może być choćby zatrucie danych.

Aleksander Czerw, Elmark Automatyka

– Z mojego punktu widzenia dla security managerów ważne jest to, żeby posługiwali się otwartymi platformami, które pozwalają na wpięcie do systemu urządzeń, które często już mają w swojej infrastrukturze od różnych producentów. Żeby nie zamykać się na to, co jest możliwe, a mieć rozwiązanie, które jest przyszłościowe.

**Wojciech Graboń,
Milestone Systems**

– Zintegrowaliśmy się z rozwiązaniem Briefcam i mamy teraz zaawansowane rozwiązania z zakresu analityki, które umożliwiają wdrażanie zaawansowanych funkcji. Oczywiście mogą w ten sposób zamieniać materiały wideo w wartościowe dane, które umożliwiają podejmowanie konkretnych i racjonalnych decyzji.

**Bartosz Wróblewski,
CCTV Baltic**

– I-pro jest pierwszy raz na Warsaw Security Summit. Na zewnątrz mamy pojazd VAN z zainstalowanymi różnego rodzaju rozwiązaniami, m.in. z kamerą i-Pro i urządzeniem amerykańskiej firmy Thermor Radar, gdzie za pomocą przetwornika termowizyjnego skanujemy obszar 360 stopni.



**Bartłomiej Bzymek,
HID Polska**

– Ta konferencja jest bardzo emocjonująca. Jest tylu specjalistów, przede wszystkim pracownicy kontrwywiadu, wielu end-userów, z którymi można przeprowadzić bardzo ciekawe dyskusje na temat tego, co się obecnie dzieje na rynku.



Jan Kapusta, CISCO

– Większość z nas przyjeżdża faktycznie po to, żeby znaleźć jakąś ciekawostkę, która czasami jest nawet w temacie, na którym się świetnie znamy, ale jest taką iskierką, która nam daje pomysł na to, co robić dalej. To jest taki dodatkowy element do tego, co już mamy całkiem fajnie zbudowane.



Tomasz Augustynowicz, CBRE

– Dużo się dzieło. Było sporo tematów związanych chociażby z przygotowaniem firm na to, żeby były odporne na zagrożenia czy zewnętrzne, czy wewnętrzne.



Paweł Pęchorzewski, Zalando

– Dużą uwagę skupialiśmy na systemach zabezpieczeń technicznych, na kamerach. Natomiast dzisiaj takim motywem przewodnim były zagrożenia hybrydowe, to jak organizacje mogą zabezpieczyć się przed właśnie tego typu zagrożeniami.



SECURITY 50:

Branża wykazuje
odporność mimo silnych
zawirowań gospodarczych

William Pao





Rok 2024 upłynął pod znakiem spowolnienia – światowa gospodarka wzrosła jedynie o 2,8% (dane Banku Światowego). Podobny trend widać w tegorocznym zestawieniu **Security 50**, gdzie średni wzrost firm sięgnął 3,28%. Mimo licznych wyzwań – od napięć handlowych po konflikty regionalne – branża security zachowuje optymizm. Przedstawiciele firm podkreślają, że kluczowym motorem rozwoju pozostaną innowacje technologiczne, zwłaszcza przełomy w dziedzinie sztucznej inteligencji.

Największe firmy

Zestawienie **asmag.com Security 50 na rok 2025** obejmuje 50 największych spółek giełdowych z branży bezpieczeństwa fizycznego, sklasyfikowanych na podstawie przychodów ze sprzedaży produktów w 2024 roku.

W pierwszej dziesiątce znalazły się: **Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Motorola Solutions, Axis Communications, Allegion, Tiandy, Hanwha Vision, Raythink i TKH.**

Hikvision i Dahua pozostają światowymi liderami – ich przychody w 2024 roku wyniosły odpowiednio **12,87 mld USD i 4,48 mld USD.**

Na liście pojawiły się także nowe firmy, m.in. Raythink, Alarm.com, Arlo i Innodet. Raythink (Chiny) specjalizuje się w inteligentnych technologiach fotoelektrycznych, natomiast koreański Innodet rozwija platformy miejskie oparte na sztucznej inteligencji.

Firmy o najwyższym wzroście

W 2024 roku **aż 33 firmy** odnotowały wzrost rok do roku. W czołówce znalazły się: **ITX, Sparsh CCTV, Dongguan Yutong Optical Technology, Tamron, Everfocus Electronics, Raythink,**

Milestone Systems, Dynacolor, Intelbras oraz Hanwha Vision. Najwięksi gracze – Hikvision i Dahua – wypadli słabiej: Hikvision zanotował wzrost o 3,5%. (wobec 7,42% rok wcześniej), a Dahua spadek o 0,1%.

Rynek chiński w dół

Słabsze wyniki chińskich firm wpłynęły negatywnie na cały rynek. Według raportu **Novaira**, globalny rynek monitoringu wizyjnego skurczył się w 2024 roku o 0,3%, głównie przez spadek w Chinach aż o 7,8%. Poza Chinami wzrost wyniósł 4,9%.

Z kolei **OMDIA** wskazuje, że chiński rynek zanotował trzeci z rzędu rok spadków – o 9,6% – podczas gdy rynki zagraniczne wzrosły o 7,5% do poziomu 16,8 mld USD.

– *Spowolnienie to efekt nałożenia się kilku czynników: kryzysu w sektorze nieruchomości, ograniczonych wydatków publicznych i niskiego zaufania biznesu, co mocno zahamowało inwestycje w sektorze rządowym i prywatnym* – wyjaśnia **Tommy Zhu**, główny analityk ds. bezpieczeństwa fizycznego w Omdia.

Omdia prognozuje jednak, że w latach 2025–2026 chiński rynek powróci do wzrostów dzięki inwestycjom w cyfryzację, infrastrukturę i nowoczesne technologie.

Burzliwy rok 2025

Nie da się ukryć – rok 2025 obfitował w wydarzenia. Wojna między Rosją a Ukrainą wciąż trwa, a konflikt na Bliskim Wschodzie zakończył się rozejmem między Izraelem a Hamasem, którego trwałość dopiero czas zweryfikuje. Jednak to nie konflikty zbrojne, lecz wojna handlowa rozpoczęta przez Stany Zjednoczone stała się siłą, która najmocniej wpłynęła na globalną gospodarkę.

2025 S50	2024 S50	NAZWA FIRMY	GŁÓWNY OBSZAR DZIAŁANIA	SIEDZIBA	PRZYCHODY W 2024 R. (MLN DOLARÓW)	WZROST PRZYCHODÓW (2024-2023)
1	1	HIKVISION DIGITAL TECHNOLOGY (monitoring wizyjny)	różne	Chiny	12866,3	3,5%
2	2	DAHUA TECHNOLOGY	różne	Chiny	4476,4	-0,1%
3	3	ASSA ABLOY (zamki mechaniczne i elektromechaniczne)	kontrola dostępu	Szwecja	4259,1	6,7%
4	5	MOTOROLA SOLUTIONS (video i analityka)	różne	USA	1920,0	11,2%
5	4	AXIS COMMUNICATIONS	różne	Szwecja	1766,9	7,4%
6	6	ALLEGION (kontrola dostępu i urządzenia elektroniczne)	kontrola dostępu	USA	943,1	-7,7%
7	7	TIANDY	monitoring wizyjny	Chiny	929,5	10,0%
8	8	HANWHA VISION	monitoring wizyjny	Korea Płd.	890,8	16,1%
9		RAYTRON (RAYTHINK)	monitoring wizyjny	Chiny	600,3	21,3%
10	9	TKH (systemy smart vision)	różne	Holandia	529,9	-2,2%
11	11	INTELBAS	różne	Brazylia	470,6	17,0%
12	10	AIPHONE	interkomy	Japonia	418,3	3,2%
13	13	DONGGUAN YUTONG OPTICAL TECHNOLOGY	monitoring wizyjny (obiektywy)	Chiny	381,6	27,9%
14	12	CP PLUS	monitoring wizyjny	Indie	366,4	9,7%
15		ALARM.COM	sygnalizacja włamania i napadu	USA	308,6	-1,2%
16	16	MILESTONE SYSTEMS	monitoring wizyjny	Dania	290,5	18,7%
17	15	ZKTECO	kontrola dostępu	Chiny	277,0	1,1%
18		ARLO	bezpieczeństwo i automatyka domowa	USA	267,9	-7,6%
19	14	VIVOTEK	monitoring wizyjny	Tajwan	228,2	-20,0%
20	17	NEDAP	różne	Holandia	163,9	-15,1%
21	19	TVT DIGITAL TECHNOLOGY	monitoring wizyjny	Chiny	161,6	7,0%
22	20	IDIS	monitoring wizyjny	Korea Płd.	148,1	0,8%
23	25	GALLAGHER	kontrola dostępu	Nowa Zelandia	123,1	5,6%
24	22	OPTEX (SECURITY SENSORS)	sygnalizacja włamania i napadu	Japonia	120,4	3,4%
25	18	NAPCO SECURITY TECHNOLOGIES	różne	USA	113,1	2,7%
26	23	INFINOVA	monitoring wizyjny	Chiny	108,1	-8,4%
27	29	MEARI	bezpieczeństwo i automatyka domowa	Chiny	103,4	10,4%
28	28	RAYSHARP	monitoring wizyjny	Chiny	94,1	0,1%
29	26	DNAKE	interkomy	Chiny	90,2	-17,7%
30	27	COMMAX	bezpieczeństwo i automatyka domowa	Korea Płd.	85,9	-0,7%
31	34	TAMRON (monitoring wizyjny i obiektywy)	monitoring wizyjny (obiektywy)	Japonia	81,4	25,8%
32	30	KOCOM	bezpieczeństwo i automatyka domowa	Korea Płd.	77,0	4,5%
33	33	SUPREMA	kontrola dostępu	Korea Płd.	73,0	11,9%
34	32	GWELLTIMES	bezpieczeństwo i automatyka domowa	Chiny	58,4	-18,7%
35		INNODEP	różne	Korea Płd.	56,8	-7,7%
36	38	DYNACOLOR	monitoring wizyjny	Tajwan	56,1	17,6%
37	35	MOBOTIX	monitoring wizyjny	Niemcy	54,1	-20,8%
38	40	SYNECTICS (dział systemów)	monitoring wizyjny	Wlk. Brytania	45,8	12,1%
39	42	SPARSH CCTV	monitoring wizyjny	Indie	41,9	28,9%
40	41	UNION BIOMETRICS (dawniej UNIONCOMMUNITY)	kontrola dostępu	Korea Płd.	41,5	10,4%
41	39	GEOVISION	monitoring wizyjny	Tajwan	37,3	-5,2%
42	43	SENSTAR TECHNOLOGIES	różne	Kanada	35,8	9,0%
43	44	HI SHARP ELECTRONICS	monitoring wizyjny	Tajwan	34,2	12,8%
44	45	C-PRO ELECTRONICS	monitoring wizyjny	Korea Płd.	27,1	8,8%
45	47	AVA GROUP	różne	Australia	15,7	6,3%
46	49	ITX AI	monitoring wizyjny	Korea	15,5	58,8%
47	48	EVERFOCUS ELECTRONICS	monitoring wizyjny	Tajwan	14,3	24,5%
48	46	ACTI	monitoring wizyjny	Tajwan	12,6	-17,1%
49	50	THRUVISION	kontrola osób	Wlk. Brytania	7,0	-29,6%
50	37	EVOLV TECHNOLOGY	Screening Systems	USA	6,5	-71,6%



Starcie gospodarcze USA z Chinami było wyjątkowo ostre – Amerykanie nałożyli potrójne cła na chińskie towary i zakazali sprzedaży zaawansowanych technologii, w tym mikroprocesorów. W odpowiedzi Chiny ograniczyły eksport metali ziem rzadkich do USA i wstrzymały zakup amerykańskiej soi. Po spotkaniu prezydentów Xi Jinpinga i Donalda Trumpa w Korei udało się jednak osiągnąć tymczasowy rozejm, który ma obowiązywać przez rok.

Mimo napięć między mocarstwami amerykańskie sankcje i cła nie odbiły się znacząco na największych chińskich firmach z branży zabezpieczeń.

– *Firmy takie jak Hikvision i Dahua rozpoczęły restrukturyzację swoich globalnych łańcuchów dostaw już w 2018 roku, gdy napięcia handlowe zaczęły narastać. Dzięki uruchomieniu produkcji w Indiach, Wietnamie i Brazylii skutecznie zminimalizowały wpływ cel – wyjaśnia Tommy Zhu, główny analityk ds. bezpieczeństwa fizycznego w Omdia.*

Jak dodaje, Hikvision stopniowo wycofał się z rynku amerykańskiego, a Dahua sprzedawała swoje rozwiązania w Ameryce Północnej, co jeszcze bardziej ograniczyło skutki nowych restrykcji. Trudniej mają mniejsi gracze, którzy polegają na sprzedaży w USA, ale nie dysponują lokalną produkcją.

Podobnego zdania jest Hikvision, który ocenia perspektywy 2025 roku pozytywnie.

– *Z naszej perspektywy rok 2025 przyniósł stabilny wzrost na rynkach międzynarodowych. Choć niektóre regiony mierzą się z wyzwaniami geopolitycznymi i handlowymi, widzimy silny popyt w krajach rozwijających się – szczególnie w regionach MEA, Ameryce Łacińskiej i Azji-Pacyfiku – mówi Allen Tang, wiceprezes Hikvision International Business Center.*

Optymizm podzielają także inni przedstawiciele branży.

– *Pomimo niepewności gospodarczej, popyt na rozwiązania bezpieczeństwa wciąż rośnie. To sektor, który od lat udowadnia swoją odporność na wahania koniunktury, a postęp technologiczny tylko*

wzmacnia tę pozycję – podkreśla Dan Kerzner, prezes Platforms Business w Alarm.com.

– *Bariery handlowe stanowią wyzwanie, zwłaszcza w obszarze transferu technologii i odporności łańcucha dostaw. W HID koncentrujemy się na potrzebach klientów, inwestujemy w lokalną produkcję i dywersyfikujemy źródła dostaw, co pozwala nam utrzymać stabilność i zaufanie klientów na całym świecie – dodaje Ramesh Songukrishnasamy, wiceprezes i CTO firmy HID.*

AI napędza rozwój branży

Zdaniem ekspertów największym motorem wzrostu w 2025 roku pozostaje sztuczna inteligencja, która zmienia sposób postrzegania bezpieczeństwa – z kosztu na inwestycję generującą wartość.

– *Integracja AI redefiniuje bezpieczeństwo fizyczne, przesuując je z poziomu reaktywnej ochrony na inteligentne, adaptacyjne systemy. Najważniejsze innowacje to te, które poprawiają świadomość sytuacyjną i umożliwiają podejmowanie decyzji w czasie rzeczywistym – mówi Howard Lang, prezes Gunnebo Entrance Control.*

Coraz większe znaczenie zyskują tzw. duże modele AI, trenowane na ogromnych zbiorach danych, które znacznie poprawiają dokładność detekcji i redukują liczbę fałszywych alarmów.

– *Duże modele AI to jedno z najbardziej przełomowych rozwiązań w branży. Od inteligentnej analizy obrazu po błyskawiczne wyszukiwanie wideo – te technologie znacząco zwiększają skuteczność ochrony, analityki biznesowej czy zarządzania ruchem. W odpowiedzi na ten trend uruchomiliśmy nasz własny model Guanlan, który zasila nową generację produktów Hikvision – mówi Allen Tang.*

Wyzwania: cyberbezpieczeństwo i kadry

Rosnące znaczenie AI przynosi też nowe ryzyka.

– *W 2025 roku obserwujemy wzrost zaawansowanych ataków opartych na AI, które zacierają granicę między cyber- a fizycznym włamaniem. Aż 62 proc. firm doświadczyło naruszeń tożsamości – wskazuje raport HID State of Security and Identity 2025.*

Branża zmaga się również z **niedoborem specjalistów** i wysoką rotacją. – *Braki kadrowe i koszty szkoleń spowalniają innowacje i utrudniają utrzymanie jakości – mówi Danille Mitchell z Gallagher Security. – Inwestujemy w edukację i partnerstwa, by wypełniać luki kompetencyjne i wspierać rozwój całej branży.*

Perspektywy na 2026

Firmy z sektora z optymizmem oceniają perspektywy na kolejne lata. Przewidywany jest dalszy wzrost rynku, napędzany rozwojem cyfrowej tożsamości, mobilnych systemów kontroli dostępu oraz biometrii. Do 2026 roku ponad 70 proc. organizacji planuje zwiększenie nakładów na rozwiązania z zakresu mobilnej identyfikacji.

Inwestycje w bezpieczeństwo utrzymują się na wysokim poziomie, a specjaliści z branży z dużym zainteresowaniem obserwują pojawiające się technologie. Sztuczna inteligencja będzie stawiała się coraz bardziej kontekstowa i silniej zintegrowana z kluczowymi obszarami, takimi jak inteligentne miasta czy infrastruktura krytyczna. Kamery zaczną pełnić funkcję zaawansowanych sensorów, dostarczających danych nie tylko w kontekście bezpieczeństwa, lecz także optymalizacji procesów biznesowych. •



Zdaniem ekspertów, największym motorem wzrostu w 2025 roku pozostaje sztuczna inteligencja, która zmienia sposób postrzegania bezpieczeństwa – z kosztu na inwestycję generującą wartość.

Witamy w świecie mechanicznych i elektronicznych systemów EVVA

Hybrydowy majstersztyk

Elektronika połączona z mechaniką w jednej wkładce - rzecz nie do podrobienia, ale do zamówienia. W EVVA!



Xesar i AirKey - elektroniczne systemy zamknięć

EVVA jest projektantem i producentem innowacyjnych elektronicznych systemów kontroli dostępu.



Arcydzieła mechaniki

Każdy system mechaniczny jest unikalny zarówno pod względem technologii jak i funkcji. Jednak wszystkie mają jedną wspólną cechę: najwyższą jakość marki.





Badanie Trendów Technologicznych 2025: Indeks Dojrzałości i Przydatności Technologii

asmag.com



W tegorocznej edycji corocznego badania asmag.com wzięło udział **ponad 200 przedstawicieli branży security**, którzy oceniali przydatność i dojrzałość kluczowych technologii stosowanych w systemach zabezpieczeń.

Ankieta objęła trzy główne kategorie: **ogólną, monitoring wizyjny oraz kontrolę dostępu**.

Niektóre rozwiązania uzyskały bardzo wysokie oceny, inne – dopiero rozwijające się – pokazują ogromny potencjał na przyszłość. Celem badania było przybliżenie technologii, które dziś i w najbliższych latach będą miały największy wpływ na rozwój branży bezpieczeństwa.

Sztuczna inteligencja dużej skali (Large-scale AI)

Sztuczna inteligencja dużej skali, trenowana na ogromnych zbiorach danych, to jeden z najgorętszych trendów w branży. W szczególności wykorzystywana jest w **chińskich systemach monitoringu wizyjnego**, które mają zapewniać **dokładniejsze wykrywanie zdarzeń, mniej fałszywych alarmów i bardziej inteligentne wyszukiwanie wideo**.

W badaniu technologia ta uzyskała jednak **umiarkowane wyniki** – **3,98 za przydatność i 3,49 za dojrzałość**. Jak zwracają uwagę eksperci, to naturalny wynik dla rozwiązania, które wciąż znajduje się na wczesnym etapie rozwoju w sektorze bezpieczeństwa.

Zdaniem specjalistów użytkownicy często postrzegają te technologie jako **jeszcze nie w pełni dojrzałe**. Jednym z głównych wyzwań jest konieczność trenowania modeli AI na dużych i różnorodnych zbiorach danych pochodzących z rzeczywistych

środowisk, co jest szczególnie trudne w obszarze systemów wysokiego bezpieczeństwa. W przypadku zastosowań krytycznych organizacje zachowują ostrożność, oczekując większej **spójności, przewidywalności i przejrzystości** działania algorytmów.

Ekspert podkreślają jednak, że w dłuższej perspektywie **potencjał dużych modeli AI jest ogromny**. Technologia ta pozwala algorytmom uczyć się z danych pochodzących z różnych lokalizacji, przypadków użycia i warunków, co w teorii czyni je znacznie bardziej **elastycznymi i kontekstowo świadomymi** niż tradycyjne modele lokalne. W praktyce wdrażanie takich systemów nadal napotyka trudności związane z **opóźnieniami, niezawodnością i cyberbezpieczeństwem**, jednak postęp w tych obszarach jest szybki.

Jak dodają przedstawiciele branży, rozwijane obecnie **modele językowo-wizyjne (VLM)** już zmieniają sposób, w jaki operatorzy pracują z danymi wideo – przekształcając złożone analizy w **proaktywne i przewidywalne wnioski**. Wraz z rozwojem infrastruktury i zasad zarządzania danymi **duże modele AI** staną się jednym z głównych motorów innowacji w sektorze bezpieczeństwa.

AI w analizie biznesowej (AI Analytics for Business Intelligence)

Zupełnie inaczej oceniono zastosowanie AI w analizie biznesowej. W tej kategorii technologia uzyskała bardzo dobre wyniki: **4,33 za przydatność i 3,87 za dojrzałość**.

AI wykorzystywana w analizie biznesowej pozwala wyciągać **praktyczne wnioski z danych wideo i innych źródeł**. Systemy te potrafią rozpoznawać obiekty i twarze, analizować zachowania czy tworzyć mapy ciepłe ruchu. Dzięki temu przedsiębiorstwa



mogą lepiej zarządzać personelem, zrozumieć zachowania klientów oraz szybciej identyfikować potencjalne ryzyka.

Eksperti zwracają uwagę, że tego typu narzędzia nie tylko podnoszą poziom bezpieczeństwa, lecz także pomagają **budować pozytywny wizerunek marki, zwiększać lojalność klientów i wspierać zrównoważony rozwój biznesu**. W efekcie popyt na tego rodzaju rozwiązania ma nadal rosnąć.

Cyberbezpieczeństwo

Najwyższe oceny w całym badaniu uzyskało **cyberbezpieczeństwo** – **4,45** za przydatność i **4,13** za dojrzałość. W czasach, gdy urządzenia są masowo połączone w sieci, a nagrania wideo mogą być łatwo zmanipulowane, znaczenie ochrony danych rośnie z każdym rokiem.

Eksperti podkreślają, że **zagrożenia związane z cyberbezpieczeństwem są dziś bardzo realne**. Rozwój narzędzi generatywnej AI umożliwia manipulowanie obrazem czy kradzież danych wideo, co stanowi poważne ryzyko dla organizacji i użytkowników. Dlatego firmy inwestują w **zaawansowane mechanizmy szyfrowania, bezpieczny rozruch systemów oraz certyfikowane standardy ochrony danych, takie jak FIPS 140-2 i FIPS 140-3**.

Jak wskazują przedstawiciele branży, rośnie też **znaczenie zgodności z regulacjami** – w tym **RODO, EU AI Act oraz NDAA**. Coraz więcej firm wprowadza zasady **privacy-by-design**, certyfikacje **ISO/IEC 27001/27701**, a także stosuje **ciągły monitoring** bezpieczeństwa w chmurze, sieci i na urządzeniach końcowych. Eksperti podkreślają, że inwestycje w cyberbezpieczeństwo nie są już jedynie wymogiem regulacyjnym – to **warunek zaufania klientów i nieprzerwanego działania systemów**.

Internet Rzeczy (IoT)

Równie wysokie noty uzyskał **Internet Rzeczy (IoT)** – **4,31** w zakresie przydatności i **4,11** w zakresie dojrzałości. Dziś trudno oddzielić bezpieczeństwo od IoT – technologie te są **ze sobą nierozdzielnie powiązane**.

Dzięki IoT branża bezpieczeństwa mogła rozwinąć się w kierunku **inteligentnych domów, budynków, transportu, handlu i miast**. Połączenie IoT z AI, określane jako **AIoT**, pozwala jeszcze

skuteczniej **zabezpieczać obiekty, analizować dane biznesowe i zwiększać efektywność operacyjną**. Zdaniem ekspertów wpływ IoT na branżę bezpieczeństwa jest ogromny i w kolejnych latach będzie tylko się zwiększał.

5G

Na wysokim poziomie oceniono również technologię **5G**, która uzyskała **4,21** za przydatność i **3,99** za dojrzałość.

Jak podkreślają specjaliści, 5G odgrywa coraz ważniejszą rolę w systemach bezpieczeństwa – umożliwia **szybszy przesył danych na większe odległości**, co sprawdza się zwłaszcza w **trudno dostępnych lokalizacjach lub przy obiektach ruchomych**.

Na rynku pojawia się coraz więcej **kamer obsługujących 5G**, a wraz z dojrzewaniem tej technologii jej znaczenie w branży bezpieczeństwa będzie systematycznie rosło.

Wnioski z badania

Na podstawie wyników badania **asmag.com Tech Trends 2025** można wyciągnąć kilka kluczowych wniosków dotyczących kierunku rozwoju branży bezpieczeństwa.

Po pierwsze, technologie oparte na **AI** – w formie zarówno dużych modeli, jak i analiz biznesowych – stopniowo dojrzewają i stają się filarem nowoczesnych systemów ochrony.

Po drugie, **cyberbezpieczeństwo** pozostaje absolutnym priorytetem, co potwierdzają najwyższe noty wśród wszystkich kategorii – firmy traktują je jako fundament zaufania i ciągłości działania.

Po trzecie, **IoT i 5G** coraz silniej kształtują sposób, w jaki rozwiązania bezpieczeństwa są projektowane i integrowane, otwierając drogę do inteligentnych, połączonych ekosystemów.

Jednocześnie widać, że część nowych technologii – **jak large-scale AI** – wciąż wymaga dopracowania i budowy zaufania użytkowników.

Ogólnie jednak branża wykazuje **dużą dojrzałość technologiczną i optymizm**, a kierunek rozwoju jest wyraźnie zorientowany na automatyzację, odporność i wartość dodaną dla biznesu. •



Kontrola dostępu 2025: rosnąca popularność mobilnych przepustek i zamków bezprzewodowych

W tegorocznej ankiecie *asmag.com* dotyczącej technologii kontroli dostępu najwyższe noty otrzymały **mobilne przepustki** – czyli rozwiązania, w których smartfon służy jako klucz do otwierania drzwi – oraz **zamki bezprzewodowe**, które łączą się z systemem zarządzania bez kabli. Coraz większym zainteresowaniem cieszą się również **biometrie multimodalne**, łączące różne metody uwierzytelniania dla zwiększenia bezpieczeństwa.

William Pao



Mobilne przepustki – telefon zamiast karty

Mobilne przepustki zdobyły mocną pozycję na rynku bezpieczeństwa w ostatnich latach. W badaniu uzyskały wysokie oceny: **4,24** za przydatność i **3,92** za dojrzałość technologiczną (w skali 1–5). Ich zalety są oczywiste – w przeciwieństwie do tradycyjnych kart czy breloków, które łatwo zgubić lub zapomnieć, **użytkownicy zawsze mają przy sobie telefon**. Wydawanie kart dostępu wiąże się też z kosztami, podczas gdy mobilną przepustkę można po prostu przesłać na urządzenie użytkownika.

Technologia stała się również bardziej zaawansowana. Wykorzystuje **Bluetooth Low Energy (BLE)**, NFC i coraz częściej **Ultra-Wideband (UWB)** – standardy obsługiwane przez wszystkie główne systemy mobilne. Co więcej, integracja z portfelami cyfrowymi, takimi jak Apple Wallet i Google Wallet, jest już standardem, co zapewnia wysoki poziom bezpieczeństwa danych. Jak podkreślają eksperci, dzięki połączeniu wygody, bezpieczeństwa

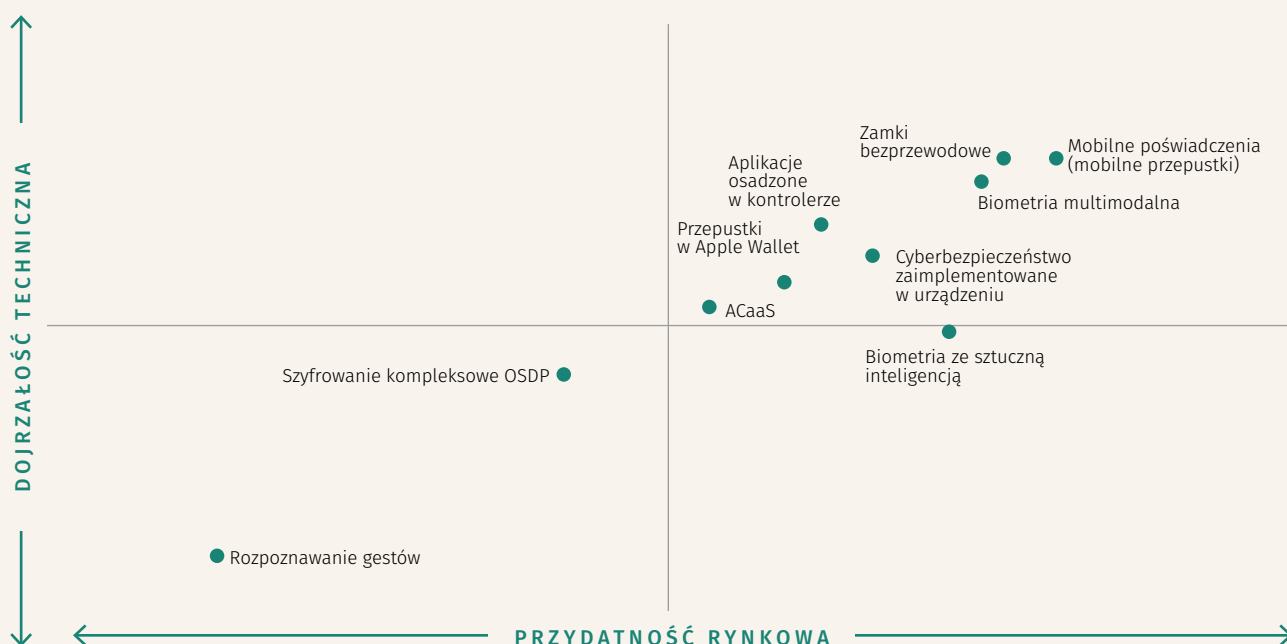
i niskich kosztów **mobilne przepustki będą nadal dynamicznie zyskiwać na popularności**.

Zamki bezprzewodowe – mniej kabli, więcej elastyczności

Kolejną wysoko ocenioną technologią są **zamki bezprzewodowe**, które w badaniu uzyskały **4,19** punktu za przydatność i **3,92** za dojrzałość technologiczną.

Zamki te komunikują się z systemem kontroli dostępu poprzez Wi-Fi, Bluetooth lub Zigbee, co eliminuje konieczność prowadzenia kabli przez ściany i drzwi. Dzięki temu instalacja jest **szybsza, tańsza i mniej inwazyjna**, szczególnie w starszych budynkach lub obiektach zabytkowych.

Zamki bezprzewodowe są także **łatwe w rozbudowie i przenoszeniu**, co sprawdza się w obiektach o zmiennym układzie pomieszczeń. Nowoczesne modele cechują się też dużą



efektywnością energetyczną – dzięki niskim poborom mocy i trybom oszczędzania energii baterie mogą działać od roku do trzech lat, w zależności od typu zamka i intensywności użytkowania.

Jak zauważają eksperci rozwój technologii bezprzewodowej i energooszczędnej sprawia, że ten segment rynku będzie rósł bardzo dynamicznie.

Biometria multimodalna – więcej niż jeden sposób weryfikacji

Biometria multimodalna, czyli uwierzytelnianie oparte na dwóch lub więcej cechach biometrycznych (np. twarz i odcisk palca), również uzyskała wysokie noty – **4,17** za przydatność i **3,87** za dojrzałość technologiczną.

Jak podkreślają eksperci, łączenie różnych metod biometrycznych **zwiększa dokładność i odporność systemu na oszustwa**, co czyni takie rozwiązania coraz bardziej popularnymi w przedsiębiorstwach i instytucjach publicznych.

Coraz częściej stosuje się też podejście, w którym dane biometryczne użytkownika **są przechowywane bezpośrednio w jego urządzeniu mobilnym**, co wzmacnia prywatność i bezpieczeństwo. Taka integracja biometrii z mobilnym dostępem staje się jednym z najbardziej praktycznych i bezpiecznych modeli autoryzacji.

Biometria wspierana przez sztuczną inteligencję

W połączeniu ze sztuczną inteligencją biometria zyskuje zupełnie nowy wymiar. W ankiecie **biometria wspierana AI** uzyskała wyniki **4,14** w przydatności i **3,59** w dojrzałości technicznej.

AI pozwala systemom rozpoznawania twarzy i odcisków palców **uczyć się zachowań użytkowników** oraz wykrywać nietypowe lub ryzykowne działania. Dzięki temu kontrola dostępu staje się bardziej proaktywna – system może reagować jeszcze przed wystąpieniem incydentu.

Jak wskazują eksperci, coraz więcej producentów **integruje sztuczną inteligencję z różnymi elementami systemów**

bezpieczeństwa – od rozpoznawania twarzy i odcisków, po analizę obrazu wideo i zarządzanie całą infrastrukturą. W efekcie rozwiązania te stają się coraz bardziej skuteczne i dopasowane do potrzeb użytkowników.

ACaaS – kontrola dostępu jako usługa

Access Control as a Service (ACaaS), czyli kontrola dostępu oferowana w modelu chmurowym, pozwala firmom zarządzać dostępem do drzwi, systemów czy danych bez konieczności utrzymywania własnych serwerów.

W ankiecie technologia ta uzyskała umiarkowane wyniki: **3,94** w przydatności i **3,63** w dojrzałości technicznej. Mimo to eksperci podkreślają, że ACaaS ma przed sobą dobrą przyszłość.

Zaletą tego rozwiązania jest **niższy koszt początkowy**, ponieważ organizacje nie muszą inwestować w drogi sprzęt. Systemy są też łatwe do skalowania – można zdalnie dodawać, usuwać lub konfigurować urządzenia oraz aktualizować polityki bezpieczeństwa w czasie rzeczywistym.

Dzięki silnemu szyfrowaniu, zgodności z normami bezpieczeństwa oraz wykorzystaniu stabilnych platform chmurowych **ACaaS staje się coraz bezpieczniejszy i bardziej dostępny**, szczególnie dla firm z wieloma lokalizacjami oraz dla małych i średnich przedsiębiorstw.

Podsumowanie

Ankieta technologiczna 2025 pokazuje wyraźny trend: **kontrola dostępu staje się coraz bardziej mobilna, bezprzewodowa i inteligentna**. Smartfony zastępują tradycyjne karty, zamki komunikują się bez kabli, a biometria – wspierana przez sztuczną inteligencję – podnosi poziom bezpieczeństwa bez utraty wygody użytkowników.

Jak podkreślają eksperci, przyszłość branży kontroli dostępu to **elastyczne, zintegrowane systemy**, które łączą bezpieczeństwo, prostotę i nowoczesne technologie w jednym ekosystemie. •



Monitoring wizyjny 2025: Edge AI i kamery wielosensorowe na czele

W najnowszej ankiecie technologicznej *asmag.com 2025* najwyższe oceny zdobyły dwie technologie – **Edge AI** (czyli sztuczna inteligencja działająca bezpośrednio w kamerze) oraz **kamery wielosensorowe**. Obydwie są coraz bardziej dojrzałe technologicznie i przynoszą realne korzyści użytkownikom.

William Pao

N

Nieco słabiej wypadły rozwiązania oparte na chmurze (VSaaS) oraz nowe technologie, takie jak wyszukiwanie nagrań w języku naturalnym czy wykrywanie wapowania.

Edge AI – sztuczna inteligencja w kamerze

Edge AI to technologia, w której wszystkie procesy analityczne – np. rozpoznawanie twarzy czy tablic rejestracyjnych – odbywają



się bezpośrednio w samej kamerze, bez potrzeby wysyłania danych do chmury czy serwera.

W ankiecie uzyskała najwyższe wyniki – **4,42** w kategorii przydatności i **4,03** w dojrzałości technicznej (w skali od 1 do 5). Jak podkreślają eksperci, to dowód na to, że rozwiązania tego typu są już w pełni sprawdzone i powszechnie stosowane.

Edge AI jest dziś cenione głównie za **praktyczność i bezpieczeństwo**. Dzięki przetwarzaniu danych lokalnie zmniejsza zużycie pasma sieciowego i koszty serwerów, a jednocześnie chroni prywatność użytkowników. Takie rozwiązania pozwalają na **błyskawiczne wykrywanie zdarzeń** i skuteczne przeszukiwanie nagrań, bez potrzeby sięgania po zewnętrzne systemy. Eksperci przewidują, że Edge AI stanie się standardem w większości nowych instalacji monitoringu.

Kamery wielosensorowe – więcej widzenia, mniej kosztów

Drugą wysoko ocenioną kategorią są **kamery wielosensorowe**, które łączą kilka obiektywów w jednym urządzeniu. Dzięki temu jedna kamera może obserwować kilka kierunków jednocześnie, co pozwala ograniczyć liczbę urządzeń i licencji.

Technologia ta zdobyła **4,18** punktu w przydatności i **3,91** w dojrzałości technicznej. Jest to szczególnie dobre rozwiązanie dla dużych przestrzeni, takich jak magazyny, hale czy parkingi.

Nowoczesne kamery wielosensorowe są coraz bardziej dopracowane – wszystkie sensory pracują w oparciu o jeden układ, co zmniejsza zużycie energii i ułatwia konfigurację. Poprawiono też jakość obrazu – nowoczesne algorytmy pozwalają płynnie łączyć obraz z kilku przetworników bez widocznych granic i różnic w oświetleniu.

VSaaS – monitoring w chmurze z ograniczeniami

Monitoring wideo jako usługa (VSaaS) otrzymał średnie wyniki – **3,98** za przydatność i **3,63** za dojrzałość techniczną. Rozwiązania chmurowe mają zalety, takie jak skalowalność i centralne zarządzanie, ale też istotne wady.

Największym problemem jest ogromne **zapotrzebowanie na przepustowość łącza**, szczególnie przy kamerach w wysokiej rozdzielczości. Dodatkowo, przetwarzanie analizy lub podgląd w czasie rzeczywistym są trudne, gdy dane muszą być przesyłane do chmury. W efekcie systemy oparte wyłącznie na chmurze są mniej praktyczne w dużych lub zdalnych instalacjach.

Coraz częściej mówi się o **rozwiązaniach hybrydowych**, które łączą zalety chmury i Edge AI – dzięki temu możliwe jest przetwarzanie danych lokalnie, przy jednoczesnym centralnym zarządzaniu systemem.

Wyszukiwanie nagrań w języku naturalnym – duży potencjał, mała dojrzałość

Nowym trendem w monitoringu jest możliwość wyszukiwania nagrań za pomocą zwykłych poleceń, np. *Pokaż osobę w czerwonej koszuli między 14:00 a 15:00*. Choć technologia ta wzbudza duże zainteresowanie, w ankiecie uzyskała umiarkowane wyniki – **3,92** w przydatności i **3,2** w dojrzałości.

Eksperci zwracają uwagę, że większość obecnych rozwiązań tego typu opiera się na chmurze, co ogranicza ich zastosowanie w branży bezpieczeństwa, gdzie wiele firm wciąż unika przesyłania wrażliwych danych wideo poza swoją infrastrukturę.

Coraz częściej opracowywane są jednak systemy, które działają **lokalnie, bez dostępu do Internetu**, zapewniając większą prywatność i bezpieczeństwo danych.

Wykrywanie wapowania – niska skuteczność i problemy z prywatnością

Po raz pierwszy w ankiecie oceniono także technologie służące do **wykrywania wapowania (e-papierosów)**. Wyniki były jednak słabe – **3,49** w przydatności i **3,09** w dojrzałości technicznej.

Powodem są ograniczenia samego monitoringu wideo. Kamery mogą łatwo pomylić parę z oddechem, dym czy odbłyśki światła z zaciągnięciem się e-papierosem, co prowadzi do wielu błędnych alarmów. Dodatkowo stosowanie kamer do tego celu może budzić **wątpliwości dotyczące prywatności**.

Eksperci wskazują, że lepszym rozwiązaniem są **specjalne czujniki dymu i pary**, które można instalować w takich miejscach, jak toalety szkolne czy korytarze, gdzie kamery nie są odpowiednie.

Podsumowanie

Wyniki ankiety jasno pokazują, że branża monitoringu coraz mocniej stawia na **lokalne przetwarzanie danych (Edge AI) i zintegrowane rozwiązania sprzętowe (kamery wielosensorowe)**. Technologie te są dojrzałe, praktyczne i pozwalają zwiększyć efektywność systemów przy jednoczesnym obniżeniu kosztów.

Z kolei rozwiązania chmurowe i eksperymentalne funkcje, takie jak wyszukiwanie w języku naturalnym czy wykrywanie wapowania, wciąż wymagają dopracowania i dostosowania do realnych potrzeb użytkowników. •





Nowe kierunki rozwoju rynku kontroli dostępu

Prasanth Aby Thomas



Europa

Europejski rynek kontroli dostępu wchodzi w fazę intensywnej transformacji napędzanej przez połączenie presji regulacyjnej, postępu technologicznego oraz rosnącego zapotrzebowania na zintegrowane systemy zarządzania budynkami.

Ramowe przepisy dotyczące prywatności – takie jak **ogólne rozporządzenie o ochronie danych (RODO)** – wraz z **rozwojem otwartych standardów komunikacji i architektur tożsamościowych (identity-first)**, przekształcają sposób projektowania, wdrażania i zarządzania systemami kontroli dostępu w całej Europie.

Dla integratorów i konsultantów bezpieczeństwa oznacza to, że sukces zależy dziś nie tylko od znajomości technologii, ale także od zrozumienia wymogów prawnych, procesów biznesowych i strategii operacyjnych klientów. Branża przesuwa się od prostych, odseparowanych rozwiązań w stronę **złożonych ekosystemów**, które łączą kontrolę dostępu z monitoringiem wizyjnym, bazami HR i automatyką budynkową.

Eksperti wskazują, że rynek ewoluuje od tradycyjnego podejścia opartego na „czytnikach i drzwiach” ku **zarządzaniu tożsamością i danymi**. Dzisiejsze trendy kształtowane są mniej przez rozwój sprzętu, a bardziej przez interpretację przepisów, interoperacyjność systemów oraz dojrzałość operacyjną przedsiębiorstw.

Trwały wpływ RODO na systemy kontroli dostępu

Europejskie przepisy o ochronie danych wciąż wywierają ogromny wpływ na projektowanie i wdrażanie systemów biometrycznych oraz mobilnych. Eksperti podkreślają, że **RODO uznaje dane biometryczne za szczególną kategorię danych**, co wymaga od organizacji jasnego określenia podstawy prawnej ich przetwarzania – zwykle poprzez wyraźną zgodę użytkownika lub uzasadniony interes.

W praktyce oznacza to, że każdy etap projektu – od planowania, przez wdrożenie, po codzienną eksploatację – musi być zgodny z rygorystycznymi zasadami prywatności. Największym

wyzwaniem nie jest sama technologia, lecz **operacyjne wdrożenie wymogów RODO** w codziennych procedurach i praktykach.

Integratorzy muszą zatem opracowywać **spójne, udokumentowane procesy**, które gwarantują zgodność z przepisami w całym cyklu życia systemu. Błędna interpretacja lub niedopilnowanie zasad może narazić użytkowników końcowych na poważne konsekwencje prawne i finansowe.

Otwarte standardy i mobilne poświadczenia przyspieszają transformację

W całej Europie coraz wyraźniej widać przejście od rozwiązań zamkniętych do **otwartych systemów komunikacji**. Szczególnie dynamicznie rozwija się standard **OSDP (Open Supervised Device Protocol)**, który zapewnia większe bezpieczeństwo, interoperacyjność i możliwości zdalnego zarządzania niż starsze technologie, takie jak Wiegand.

Choć wdrożenie OSDP wiąże się z nieco wyższymi kosztami i wymaga większej wiedzy technicznej od instalatorów, eksperci zwracają uwagę, że **długoterminowe korzyści** – w tym krótszy czas instalacji i niższe koszty utrzymania – rekompensują te początkowe wyzwania.

Równolegle dynamicznie rośnie popularność **mobilnych poświadczeń**, które umożliwiają użytkownikom dostęp za pomocą smartfonów. Takie rozwiązania wspierają modele pracy hybrydowej i zarządzanie wieloma lokalizacjami jednocześnie, oferując elastyczność, wygodę i większe bezpieczeństwo dzięki możliwości natychmiastowego nadawania i cofania uprawnień.

Integracja wykracza poza tradycyjne systemy bezpieczeństwa

W 2025 roku pojęcie „integracji systemów” nabiera nowego znaczenia. Coraz częściej integratorzy muszą łączyć systemy zabezpieczeń technicznych z **narzędziami zarządzania budynkiem i procesami operacyjnymi przedsiębiorstwa**.

Eksperti podkreślają, że skuteczne projekty nie mogą ograniczać się do aspektów technicznych, lecz muszą być **ukierunkowane na konkretne rezultaty biznesowe** – takie jak płynność ruchu osób, bezpieczeństwo, zgodność z przepisami, efektywność energetyczna czy poprawa doświadczeń użytkowników.

To podejście prowadzi do **integracji systemów**, w której kontrola dostępu, monitoring wizyjny i zarządzanie tożsamością są

połączone z systemami HR, HVAC, aplikacjami biurowymi i platformami zarządzania gośćmi.

Coraz większą rolę odgrywa też **architektura zorientowana na tożsamość (identity-first)**, w której tożsamość użytkownika staje się centralnym elementem projektu systemu, a wszystkie pozostałe rozwiązania są do niej dopasowywane.

Wyzwania operacyjne i prywatność

Europejskie regulacje dotyczące ochrony danych pozostają dużym wyzwaniem dla wielu firm integracyjnych. Eksperti podkreślają, że **zgodność z przepisami musi być częścią kultury organizacyjnej, a nie jedynie formalnością**.

Kluczem jest budowanie wspólnego zrozumienia przepisów w zespołach oraz tworzenie powtarzalnych, dobrze udokumentowanych procedur obejmujących każdy etap projektu – od wymagań i projektowania, przez uruchomienie, po konserwację, audyty i reagowanie na incydenty.

Sektory napędzające rozwój: centra danych i infrastruktura krytyczna

Wśród branż, które najintensywniej inwestują w nowoczesne systemy kontroli dostępu, dominują **centra danych i przedsiębiorstwa infrastruktury krytycznej**.

Eksperti wskazują, że najbardziej zaawansowani klienci koncentrują się dziś nie na urządzeniach, ale na **zarządzaniu tożsamością w rozproszonych środowiskach**.

Centra danych, ze względu na skalę i wrażliwość przetwarzanych informacji, wymagają bezbłędnej identyfikacji użytkowników i zgodności z rygorystycznymi protokołami bezpieczeństwa. Z kolei firmy z sektora infrastruktury krytycznej muszą zapewniać

bezpieczny dostęp dla rotujących zespołów technicznych i podwykonawców na rozproszonych geograficznie obiektach.

W obu przypadkach kluczowe staje się zarządzanie **cyklem życia tożsamości oraz interoperacyjność między różnymi systemami i lokalizacjami**.

Trendy w 2025 roku

Europejski rynek kontroli dostępu w 2025 roku jest coraz mocniej definiowany przez **integrację, świadomość prywatności oraz konwergencję IT i bezpieczeństwa fizycznego**.

Integratorzy odchodzą od podejścia produktowego na rzecz **modelu usługowego**, w którym kluczowe znaczenie mają rezultaty biznesowe i cele zrównoważonego rozwoju.

Szybkie tempo adopcji standardu OSDP oraz mobilnych poświadczeń wyznacza fundament dla **inteligentnych, tożsamościowo zorientowanych środowisk**. Jednak powodzenie tej transformacji będzie zależać od zdolności integratorów do wdrożenia zgodności regulacyjnej, podnoszenia kompetencji technicznych zespołów i lepszego zrozumienia procesów klientów.

Eksperti przewidują, że firmy, które potrafią patrzeć szerzej – wychodząc poza sprzedaż systemów i koncentrując się na **rozwiązywaniu kompleksowych problemów operacyjnych** – staną się liderami kolejnej fali innowacji w europejskiej kontroli dostępu.

Dla integratorów i konsultantów rok 2025 nie będzie już tylko okresem wdrażania nowych technologii, lecz czasem budowania **zintegrowanych, zgodnych z regulacjami i opartych na tożsamości ekosystemów**, które zwiększają bezpieczeństwo, efektywność operacyjną i wartość biznesową organizacji. •



meryka Północna

Rynek kontroli dostępu w Ameryce Północnej w 2025 roku wchodzi w nową fazę transformacji. Zmiany te napędza połączenie technologii **chmurowych, sztucznej inteligencji (AI) oraz rozwiązań mobilnych**, które radykalnie zmieniają sposób zarządzania bezpieczeństwem i świadczenia usług przez integratorów systemów.

Według prognoz firmy MarketsandMarkets globalny rynek kontroli dostępu ma wzrosnąć z **10,62 mld USD w 2025 roku do 15,8 mld USD w 2030**, a głównym motorem wzrostu będą platformy oparte na chmurze i analityka wspierana AI.

AI i chmura przekształcają operacje

Jak podkreślają eksperci, branża przechodzi widoczną transformację – tradycyjne, ręczne konfiguracje i sztywne struktury ustępują miejsca inteligentnym platformom dostępu, które oferują dane w czasie rzeczywistym i coraz większy poziom automatyzacji.

Technologia chmurowa umożliwia dziś **centralne zarządzanie dostępem**, natychmiastowe aktualizacje, nieprzerwaną dostępność

i pełną widoczność procesów – co jest kluczowe przy skalowaniu bezpieczeństwa w organizacjach wielooddziałowych.

Połączenie chmury z AI sprawia, że systemy kontroli dostępu stają się **proaktywne**, potrafiąc przewidywać zagrożenia, reagować na nie natychmiast i adaptować się do zmieniających się warunków bez zakłóceń. Dzięki temu operatorzy mogą skupić się na incydentach o największym znaczeniu, zamiast przeglądać setki logów ręcznie.

Mobilny dostęp i tożsamość w centrum uwagi

Rosnąca popularność **mobilnych identyfikatorów** odzwierciedla oczekiwania użytkowników, by bezpieczeństwo było równie wygodne jak inne aspekty życia cyfrowego. Eksperti zauważają, że pracownicy coraz częściej korzystają z telefonów do komunikacji, płatności i potwierdzania tożsamości – dlatego rozwiązania mobilne stają się naturalnym elementem systemów dostępu.

Systemy oparte na tożsamości i urządzeniach mobilnych pozwalają organizacjom **wydawać, zarządzać i unieważniać uprawnienia w czasie rzeczywistym**, a wbudowane zabezpieczenia – takie jak biometryka czy kody dostępu – zwiększają poziom zaufania przy każdej interakcji. Dodatkowo, takie poświadczenia są łatwo przenośne i integrują się z platformami chmurowymi, co zapewnia spójność uprawnień w wielu lokalizacjach.



Cyberbezpieczeństwo – fundament współczesnej ochrony

W dobie połączonych systemów granica między bezpieczeństwem fizycznym a cyfrowym praktycznie się zatarła. Coraz większa liczba urządzeń i danych wymaga **zintegrowanych ram bezpieczeństwa**, które chronią jednocześnie ludzi i informacje.

Nowoczesne systemy są projektowane tak, by **wykrywać zagrożenia niezależnie od ich źródła** – czy chodzi o fizyczne wtargnięcie, czy o próbę naruszenia sieci. Cyberbezpieczeństwo stało się kluczowym kryterium przy wyborze dostawców i integratorów, wpływając na decyzje zakupowe, zgodność z przepisami i strategię wdrożeniową.

Firmy inwestują w **certyfikowane rozwiązania, szyfrowanie danych, bezpieczne aktualizacje i zgodność z regulacjami**, aby chronić infrastrukturę i budować zaufanie klientów.

Nowe modele usług i integracji

Przejęcie na rozwiązania chmurowe zmienia także model biznesowy integratorów. Zamiast jednorazowych wdrożeń coraz częściej oferują oni **usługi zarządzane i abonamentowe**, które zapewniają stałe przychody i długoterminowe relacje z klientami.



zja

Rynek kontroli dostępu w Azji rośnie w szybkim tempie, a transformacja cyfrowa zasadniczo zmienia sposób, w jaki organizacje zarządzają bezpieczeństwem fizycznym. Połączenie **sztucznej inteligencji (AI), biometrii, mobilnych poświadczeń i platform zarządzanych w chmurze** sprawia, że coraz więcej firm wdraża nowoczesne systemy dostępu, które łączą bezpieczeństwo, efektywność i zgodność z regulacjami.

Według danych Grand View Research rynek kontroli dostępu w regionie Azji i Pacyfiku osiągnął w 2024 roku wartość **3,38 mld USD**, a do 2030 roku ma wzrosnąć do **6,15 mld USD**, przy średniorocznym tempie wzrostu wynoszącym **10,6%**. Dynamiczny rozwój wynika głównie z postępującej **urbanizacji** oraz ambitnych programów **smart city** w Chinach, Indiach, Singapurze i Korei Południowej, gdzie inwestycje w infrastrukturę cyfrową stale się zwiększają.

Eksperti podkreślają, że **Azja jest dziś liderem globalnej transformacji cyfrowej**, a jej rynek kontroli dostępu redefiniuje

Integratorzy poszerzają kompetencje o **zarządzanie usługami w chmurze, zdalne monitorowanie i analitykę**, co pozwala im świadczyć wsparcie ciągłe i zwiększać rentowność. Dzięki temu projekty przekształcają się w **stałe partnerstwa oparte na subskrypcji**, a biznes staje się bardziej odporny i przewidywalny.

Generatywna AI i decyzje oparte na danych

Patrząc w przyszłość, rola sztucznej inteligencji w kontroli dostępu będzie tylko rosła. **Generatywna AI** stanie się kluczowym trendem – umożliwiając analizę ogromnych ilości danych z połączonych systemów i wspierając operatorów w szybkim podejmowaniu decyzji.

Systemy oparte na AI pozwolą **identyfikować wzorce zachowań, wykrywać anomalie i reagować w czasie rzeczywistym**, zwiększając autonomię i skuteczność działań.

Integracja urządzeń w ramach jednej platformy stworzy spójne środowisko, w którym dane staną się źródłem inteligentnych rekomendacji i predykcji.

Wnioski: rynek coraz bardziej zintegrowany i zrównoważony

Jak podkreślają eksperci, rok 2025 wyznacza nowy etap w rozwoju rynku kontroli dostępu w Ameryce Północnej. **AI, chmura, mobilny dostęp i cyberbezpieczeństwo** nie są już trendami, lecz podstawowymi elementami nowoczesnych systemów bezpieczeństwa.

Integratorzy, którzy inwestują w dane, kompetencje chmurowe i zgodność regulacyjną, będą odgrywać kluczową rolę w tworzeniu inteligentnych, połączonych i zrównoważonych ekosystemów bezpieczeństwa przyszłości. •

standardy bezpieczeństwa fizycznego dzięki synergii biometrii, AI, technologii mobilnych i chmurowych.

AI podnosi dokładność i niezawodność systemów

Sztuczna inteligencja staje się głównym motorem innowacji w obszarze biometrycznej kontroli dostępu. Algorytmy oparte na **uczeniu głębokim** pozwalają analizować miliony punktów danych w czasie rzeczywistym, co umożliwia szybsze i bardziej precyzyjne rozpoznawanie użytkowników oraz dostosowywanie się do czynników środowiskowych, takich jak oświetlenie, kąt twarzy czy ruch.

Dzięki AI systemy biometryczne osiągają nowy poziom **dokładności i adaptacyjności**, minimalizując błędne odrzucenia i podnosząc ogólną wydajność. Technologie te są coraz częściej stosowane w środowiskach wymagających maksymalnej precyzji – takich jak lotniska, szpitale czy instytucje rządowe o wysokim poziomie zabezpieczeń.

Dla integratorów rozwój AI otwiera nowe możliwości oferowania **inteligentnych i odpornych systemów**, łączących wiele metod uwierzytelniania – od rozpoznawania twarzy i linii papilarnych po mobilne identyfikatory.

Mobilność i chmura zmieniają zarządzanie systemami

Obok sztucznej inteligencji to właśnie **mobilne poświadczenia** oraz **platformy chmurowe** wywierają największy wpływ na rynek azjatycki. Coraz częściej tradycyjne karty i identyfikatory zastępowane są przez uwierzytelnianie przy użyciu smartfonów.

Równocześnie systemy oparte na chmurze umożliwiają administratorom **zdalne zarządzanie uprawnieniami, monitorowanie aktywności oraz aktualizacje systemów w czasie rzeczywistym**.

Ten trend napędza **zapotrzebowanie na otwarte platformy API i SDK**, które umożliwiają interoperacyjność z systemami zewnętrznymi. Dla integratorów oznacza to szansę na tworzenie **skalowalnych, elastycznych i spersonalizowanych rozwiązań**, dostosowanych do indywidualnych potrzeb klientów.

Ochrona danych i regulacje kształtują nowe standardy

Dynamicznie zmieniające się regulacje dotyczące ochrony danych w Azji mają coraz większy wpływ na projektowanie i wdrażanie systemów kontroli dostępu. Kraje takie jak **Japonia i Korea Południowa** zbliżają swoje przepisy do europejskiego **RODO**, a **Indie** wprowadziły własną ustawę o ochronie danych osobowych (*Digital Personal Data Protection Act*).

Przedsiębiorstwa coraz częściej wdrażają zasadę „**privacy by design**”, czyli projektowania systemów z uwzględnieniem prywatności użytkownika już od etapu koncepcji. Obejmuje to m.in. przetwarzanie danych biometrycznych lokalnie, bez przysyłania ich do centralnych serwerów, a także szyfrowanie i bezpieczne przechowywanie danych.

Coraz więcej producentów stosuje tzw. **edge processing**, dzięki któremu dane biometryczne są przetwarzane i przechowywane bezpośrednio w urządzeniu, co minimalizuje ryzyko naruszenia prywatności i ułatwia zgodność z lokalnymi przepisami.

Eksperti podkreślają, że **zgodność z regulacjami** staje się dziś nie tylko wymogiem prawnym, ale również **przewagą konkurencyjną**, ponieważ instytucje publiczne i prywatne coraz częściej wybierają rozwiązania gwarantujące pełną transparentność i kontrolę nad danymi.

Cyberbezpieczeństwo i zgodność ze standardami w centrum uwagi

W obliczu rosnących zagrożeń cybernetycznych producenci i integratorzy przywiązują coraz większą wagę do **międzynarodowych norm i certyfikacji**, takich jak **ISO/IEC 27001** (zarządzanie bezpieczeństwem informacji) czy **ISO/IEC 27701** (zarządzanie prywatnością danych).

Jak wskazują eksperci, przestrzeganie tych standardów jest dziś kluczowe dla zapewnienia zaufania klientów i niezawodności produktów.

Firmy wiodące na rynku wdrażają te normy zarówno na etapie projektowania, jak i eksploatacji systemów, a ich urządzenia uzyskują również certyfikaty, takie jak **CE RED**, potwierdzające zgodność z wymogami cyberbezpieczeństwa dla urządzeń IoT.

W całej branży obserwuje się wyraźny trend w kierunku **pełnej zgodności z regulacjami międzynarodowymi** – w tym z europejskim RODO, aktem AI Act czy wymogami NDAA – co

gwarantuje, że oferowane rozwiązania są nie tylko nowoczesne technologicznie, ale także gotowe do globalnego wdrożenia.

Integracja jako kluczowy kierunek rozwoju

Rosnące zapotrzebowanie na interoperacyjność zmienia podejście integratorów do projektowania systemów. Coraz więcej przedsiębiorstw oczekuje **zunifikowanych platform bezpieczeństwa**, które łączą kontrolę dostępu z monitoringiem wideo, analityką i narzędziami operacyjnymi.

Takie zintegrowane środowiska zapewniają **większą widoczność procesów, centralne zarządzanie i możliwość analizy danych w ujęciu całościowym**.

Dla integratorów kluczowym czynnikiem sukcesu staje się **otwarta architektura**, pozwalająca na łatwą integrację z różnymi systemami sprzętowymi i programowymi. W regionie Azji i Pacyfiku – gdzie rozwój przedsiębiorstw i miast inteligentnych postępuje wyjątkowo dynamicznie – taka elastyczność jest szczególnie istotna dla długowieczności i skalowalności systemów.

Trendy kształtujące przyszłość rynku

Analitycy przewidują, że do 2026 roku rynek kontroli dostępu w Azji będzie nadal dynamicznie się rozwijał, napędzany przez **AI, analitykę danych i integrację tożsamości cyfrowych**.

Coraz większe znaczenie zyskuje również **zrównoważony rozwój**, obejmujący optymalizację zużycia energii i zasobów dzięki inteligentnemu zarządzaniu budynkami i rozwiązaniom chmurowym.

Równocześnie rządy planują **wzmocnienie regulacji dotyczących prywatności i bezpieczeństwa IoT**, co wpłynie na sposób projektowania i wdrażania systemów w nadchodzących latach.

Eksperti przewidują, że **kolejna faza wzrostu rynku** będzie zależeć od tego, jak skutecznie dostawcy technologii i integratorzy dostosują się do tych zmian. Szybki rozwój AI i jej zastosowanie w bezpieczeństwie zdefiniuje na nowo możliwości organizacji i całych społeczności.

Perspektywy dla integratorów i doradców

Dla integratorów systemów bezpieczeństwa nowa rzeczywistość – oparta na AI, ochronie prywatności i interoperacyjności – niesie zarówno **szanse, jak i wyzwania**.

Sukces na tym rynku wymaga dziś wiedzy nie tylko z zakresu instalacji sprzętu, ale także **zarządzania danymi, architektury systemów i cyberbezpieczeństwa**.

Firmy, które potrafią dostarczyć **zintegrowane, zgodne ze standardami i regulacjami rozwiązania**, będą najlepiej przygotowane do sprostan rosnącym wymaganiom klientów.

Umiejętność połączenia lokalnych przepisów, globalnych norm oraz indywidualnych potrzeb operacyjnych klientów stanie się kluczem do zdobywania projektów w coraz bardziej konkurencyjnym środowisku.

Rynek kontroli dostępu w regionie **Azji i Pacyfiku** utrzymuje silną dynamikę wzrostu, potwierdzając swoją rolę jako **globalnego centrum innowacji w zakresie bezpieczeństwa fizycznego**. Integracja sztucznej inteligencji, biometrii i technologii chmurowych przekształca kontrolę dostępu w strategiczne narzędzie transformacji cyfrowej, otwierając nową erę dla dostawców technologii i organizacji, które z nich korzystają. •



Co kształtuje rynek monitoringu wizyjnego

Prasanth Aby Thomas



Europa

Rynek monitoringu wizyjnego w Europie w 2025 roku rozwija się pod wpływem dwóch głównych czynników: coraz bardziej szczegółowych regulacji (takich jak RODO czy unijna ustawa o AI) oraz rosnącej popularności hybrydowych systemów opartych na sztucznej inteligencji, które muszą łączyć skuteczność z poszanowaniem prywatności.

Dla integratorów i doradców systemów zabezpieczeń oznacza to całkowite przeprojektowanie sposobu, w jaki powstają, działają i są oceniane rozwiązania technologiczne.

Regulacje napędzają odpowiedzialne innowacje

Wpływ RODO na monitoring wizyjny jest dziś dobrze znany. Przepisy, które początkowo koncentrowały się na ochronie prywatności, stały się fundamentem etycznego podejścia do danych w całej

branży. Jak wyjaśniają eksperci z Axis Communications, RODO podniosło poprzeczkę i nadal definiuje zasady przetwarzania, przechowywania i zabezpieczania danych.

Dojrzałość RODO mocno wpływa też na rozwój analityki opartej na AI. Dzisiejsze systemy potrafią rozpoznawać zachowania, klasyfikować pojazdy czy analizować cechy demograficzne – ale to wymaga ogromnych i odpowiednio przygotowanych zbiorów danych. Unijna ustawa o sztucznej inteligencji wymusza więc pytania o to, skąd te dane pochodzą, czy są etycznie pozyskane i czy nie zawierają ukrytych uprzedzeń.

Jak podkreślają eksperci, takie pytania mają zapobiegać nadużyciom i dyskryminacji. Przypominają, że to reakcja na lata kontrowersji związanych z nieetycznym wykorzystaniem danych – od Cambridge Analytica po przypadki nielegalnego profilowania.

Ekspert z Axis zauważają również, że regulacje nie blokują innowacji, ale je porządkują i kierunkują. RODO i ustawa o AI tworzą ramy, w których technologie muszą być projektowane od początku tak, by uwzględniały prywatność, prawa człowieka i pełną przejrzystość działania. Zwiększa to też zaufanie klientów – użytkownicy wiedzą, że jeśli dostawca technologii nie spełni wymogów etycznych, konsekwencje mogą być poważne.

Również inni producenci, tacy jak MOBOTIX, wskazują, że zgodność z regulacjami stała się przewagą konkurencyjną. Według ekspertów firmy RODO i ustawa o AI przyspieszają rozwój odpowiedzialnych technologii, a „prywatność wbudowana w projekt” pozostaje ważnym filarem europejskich rozwiązań.

AI, chmura i systemy hybrydowe w natarciu

Sztuczna inteligencja staje się kluczowym elementem współczesnych systemów monitoringu w Europie. Jak podkreślają eksperci, firmy coraz chętniej wdrażają AI ze względu na jej praktyczną użyteczność, zwłaszcza w zarządzaniu dużą liczbą kamer i szybkim przeszukiwaniu nagrań.

Przykłady takich narzędzi pokazują, że operatorzy mogą dziś wpisać prosty opis – np. „żółty van dostawczy” albo „mężczyzna w niebieskiej czapce” – i w kilka sekund znaleźć odpowiednie nagranie.

Jednak eksperci zwracają uwagę, że użytkownicy nadal potrzebują edukacji. Wiele osób wciąż podchodzi do AI z nieufnością, dlatego producenci powinni jasno wyjaśniać zarówno zalety, jak i ograniczenia tych technologii. Obecnie rola mocy obliczeniowej bywa niedoceniana. Zaawansowane analityki mogą obciążać serwery, chyba że zastosuje się specjalistyczny sprzęt lub analityki działające na krawędzi sieci (*edge*).

Równolegle rośnie adopcja systemów chmurowych i hybrydowych. Jak wyjaśniają eksperci, przejście do chmury w Europie jest bardziej stopniowe niż przewidywano kilka lat temu, ale technologie „kamera do chmury” już dziś znajdują zastosowanie w wielu projektach.

Najpopularniejszym modelem wciąż pozostaje hybryda – łączenie nagrywania lokalnego z usługami chmurowymi. Według ekspertów pozwala to ograniczyć koszty, zachować kontrolę i zwiększyć odporność na awarie.

Równowaga między analizą a zgodnością

Rynek europejski jest wyjątkowo wrażliwy na kwestie prywatności i zgodności z prawem, nawet przy rosnącym zapotrzebowaniu

na zaawansowaną analitykę. Jak podkreślają eksperci, klienci chcą innowacji, ale nie kosztem zgodności z przepisami. Producentom udaje się to osiągnąć dzięki zdecentralizowanej analizie danych wykonywanej bezpośrednio w kamerach, co minimalizuje przesyłanie danych osobowych. Jak wyjaśniają eksperci, zaawansowane analizy – takie jak wykrywanie zachowań czy klasyfikacja obiektów – mogą działać w sposób zgodny z RODO, jeśli większość przetwarzania odbywa się na urządzeniu.

Ekspert Axis dodają, że regulacje stały się dziś częścią procesu projektowania technologii od pierwszego etapu. Integratorzy nie mogą już traktować zgodności jako „ostatniego kroku” – muszą uwzględnić ją na poziomie architektury systemu.

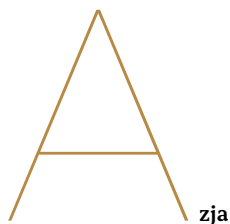
Co dalej dla integratorów i doradców?

Europejski rynek monitoringu w 2025 roku zmierza w stronę odpowiedzialnej inteligencji – połączenia zaawansowanej technologii z etycznym podejściem do danych. AI poprawia efektywność, hybrydy pozwalają skalować systemy, a regulacje wyznaczają granice, w których można bezpiecznie działać.

Jak wskazują eksperci, rozwiązania hybrydowe prawdopodobnie pozostaną dominującym modelem, bo łączą niezawodność, elastyczność i skalowalność.

Z kolei według innych ekspertów, to zaufanie i odpowiedzialność staną się głównymi wyróżnikami rynkowymi – ustawa o AI będzie premiować technologie, które potrafią połączyć inteligencję z transparentnością.

Rezultatem jest europejski krajobraz bezpieczeństwa, w którym prywatność i efektywność nie konkurują ze sobą, ale wspólnie tworzą podstawę nowoczesnych, świadomych rozwiązań monitoringu. •



zja

Rynek monitoringu wizyjnego w Azji przechodzi dużą transformację. Jak podkreślają eksperci, sztuczna inteligencja, regulacje dotyczące prywatności oraz hybrydowe architektury chmurowo-edge zmieniają sposób projektowania i wdrażania systemów. Wzrost liczby inteligentnych miast, automatyzacja przemysłu i rosnące wymagania bezpieczeństwa przyspieszają przesunięcie od tradycyjnego monitoringu do systemów analitycznych, które wspierają decyzje biznesowe i operacyjne.

Dla integratorów i konsultantów oznacza to zarówno szanse, jak i wyzwania. Klienci coraz częściej oczekują, że monitoring wizyjny nie tylko zapewni bezpieczeństwo, lecz także dostarczy informacji w czasie rzeczywistym, poprawi efektywność operacyjną i wspomże podejmowanie decyzji, przy jednoczesnym przestrzeganiu coraz bardziej rygorystycznych przepisów o ochronie danych.

AI jako serce monitoringu

Według ekspertów z VIVOTEK analityka wizyjna oparta na AI przestaje być tylko „dodatkową funkcją bezpieczeństwa” i staje się platformą biznesową. Organizacje w całej Azji szukają inteligentnych systemów, które dostarczą wglądu w czasie rzeczywistym, umożliwią analizę zachowań, wykrywanie obiektów, rozpoznawanie twarzy czy wykrywanie anomalii – wszystko po to, aby zwiększyć bezpieczeństwo, efektywność i wspierać podejmowanie decyzji.

Jak podkreślają eksperci, rosnące wykorzystanie AI w monitoringu odpowiada na potrzeby azjatyckich firm i władz – systemy nie tylko wykrywają intruzów czy kontrolują dostęp, lecz także optymalizują operacje w sklepach, monitorują bezpieczeństwo w fabrykach i wspierają zarządzanie ruchem miejskim. Szybka urbanizacja i rozwój inteligentnych miast dodatkowo zwiększają popyt na systemy edge AI, a chmura staje się coraz popularniejsza w rozwiązaniach elastycznych i zdalnie zarządzanych. Klienci coraz częściej oczekują integracji z IoT, centralnego zarządzania i niższych kosztów utrzymania – co stawia AI w roli kluczowego elementu nowoczesnej analityki wideo.



Hybrydowe architektury

Wraz z upowszechnieniem sztucznej inteligencji zmieniają się też modele infrastruktury. Eksperti zwracają uwagę, że chmura i edge AI działają teraz wspólnie: analiza w czasie rzeczywistym odbywa się na urządzeniach końcowych, a chmura zapewnia skalowalność, centralne zarządzanie i głębsze analizy w wielu lokalizacjach.

Hybrydowe systemy pozwalają łączyć szybkość i inteligencję: kluczowe analizy mogą działać lokalnie, a dane długoterminowe i wnioski są konsolidowane w chmurze. To rozwiązanie sprawdza się szczególnie w dużych, wielostanowiskowych wdrożeniach, takich jak sieci transportowe, kompleksy przemysłowe czy miejskie centra dowodzenia.

Eksperti podkreślają, że hybrydowe architektury stają się coraz bardziej popularne w Azji, zwłaszcza przy rozwoju inteligentnych miast, transportu i przemysłu. Integratorzy muszą projektować systemy, które dynamicznie rozdzielają obciążenia między edge a chmurę, zapewniając przy tym wysoki poziom wydajności i elastyczność.

Prywatność i zgodność z przepisami

Szybkie wdrażanie AI w Azji idzie w parze z rosnącym znaczeniem prywatności i zgodności z prawem. Wiele krajów wprowadza surowsze regulacje dotyczące gromadzenia, przechowywania i przetwarzania danych wideo. To sprawia, że systemy edge AI, które przetwarzają dane bezpośrednio na kamerze, szyfrują je i stosują precyzyjnie określone uprawnienia dostępu, stają się preferowanym rozwiązaniem.

Eksperti podkreślają, że prywatność i zgodność stają się integralną częścią projektowania systemów, a nie dodatkiem „na końcu procesu”. Rozwiązania muszą być inteligentne, wydajne i prawnie bezpieczne już od momentu wdrożenia.

Wpływ regulacji europejskich

Choć ramy prywatności w Azji różnią się w zależności od kraju, eksperci wskazują, że wiele państw i dostawców technologii bacznie obserwuje regulacje europejskie, takie jak RODO i unijna ustawa o AI. Europejskie doświadczenia pokazują, że innowacja może współistnieć z regulacjami: prywatność, prawa człowieka i transparentność nie są przeszkodą, są wbudowane w proces od początku.

To podejście powoli wpływa też na azjatyckich użytkowników, którzy coraz większą wagę przykładają do transparentności

danych i etycznego treningu algorytmów AI. Dla globalnych integratorów oznacza to konieczność znajomości zarówno lokalnych przepisów, jak i światowych standardów najlepszych praktyk.

Balans między wydajnością AI a efektywnością systemu

Zaawansowane algorytmy AI wymagają dużej mocy obliczeniowej, co może zwiększać koszty sprzętu i złożoność systemu. W Azji szczególnie nacisk kładzie się na efektywność kosztową i skalowalność – dlatego integratorzy wykorzystują *edge computing* i zoptymalizowany sprzęt, by zapewnić wysoką wydajność bez obciążania sieci i chmury.

Rozwiązania hybrydowe i *edge-based* gwarantują szybkie reakcje w czasie rzeczywistym, kontrolę kosztów pasma oraz zgodność z lokalnymi wymogami dotyczącymi przetwarzania danych. Dzięki temu architektury są elastyczne i mogą rosnąć wraz z potrzebami – od małych sieci handlowych po nadzór całych miast.

Co to oznacza dla integratorów i konsultantów

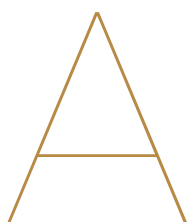
Projektowanie systemów monitoringu wizyjnego wymaga teraz wiedzy wykraczającej poza instalację sprzętu. Trzeba uwzględniać, gdzie przetwarzane są dane, jak trenowane są analityki AI i jakie przepisy wpływają na strategię wdrożenia.

Klienci oczekują dziś większej transparentności i odpowiedzialności. Integratorzy muszą zapewnić, że systemy są skonfigurowane poprawnie, spełniają lokalne przepisy i pozwalają równoważyć innowacje z zgodnością prawną.

Perspektywy: ku zaufanej inteligencji

W miarę dojrzewania rynku monitoringu w Azji, wzrost będzie zależał nie tylko od wydajności systemów AI i chmurowych, lecz także od poziomu zaufania, jaki budzą. Jak zauważają eksperci, integratorzy i konsultanci, którzy potrafią projektować systemy inteligentne, szanujące prywatność i działające w architekturze *edge*, najlepiej wykorzystają rozwój inteligentnej infrastruktury w regionie.

Regulacje w Singapurze, Indie wprowadzające nowe prawo ochrony danych czy japońskie inicjatywy *edge computing* pokazują, że Azja zmierza w stronę systemów monitoringu, które są zarówno inteligentne, jak i odpowiedzialne. Eksperti podkreślają, że równowaga między AI, prywatnością i zaufaniem zdefiniuje kolejny etap rozwoju rynku. •



meryka Północna

Rynek monitoringu wizyjnego w Ameryce Północnej przechodzi obecnie ogromną zmianę. Dzięki szybkiemu rozwojowi sztucznej inteligencji, chmury i integracji systemów branża bezpieczeństwa odchodzi od zwykłego nagrywania obrazu na rzecz inteligentnych, zautomatyzowanych rozwiązań, które pomagają podejmować decyzje i optymalizować pracę firm.

Monitoring nie polega już tylko na patrzeniu w ekrany. Teraz liczy się analiza, automatyczne reakcje i współpraca systemów w całej organizacji.

Jak zauważyli eksperci, rok 2025 to moment, w którym AI i chmura zaczynają realnie zmieniać codzienną pracę firm: przyspieszają podejmowanie decyzji, ułatwiają zarządzanie infrastrukturą i pozwalają budować bardziej elastyczne, przewidywalne systemy bezpieczeństwa.

AI i chmura wchodzą do mainstreamu

Zarówno sztuczna inteligencja, jak i rozwiązania chmurowe zyskują ogromną popularność, bo organizacje chcą pracować szybciej i oszczędniej. Firmy coraz częściej wybierają podejście hybrydowe – część systemu działa lokalnie, część w chmurze, a przejście między tymi modelami można wykonać stopniowo.

W bankowości i finansach to szczególnie widoczne: jak zauważyli eksperci, instytucje testują nowe rozwiązania, które upraszczają codzienną pracę, nie rezygnując z kontroli nad lokalnymi systemami. Dzięki temu mogą modernizować się krok po kroku i na bieżąco oceniać efekty.

Monitoring staje się inteligentny

Zmiany w branży następują wyjątkowo szybko. AI i chmura tworzą teraz fundament nowoczesnych systemów, które potrafią nie tylko nagrywać obraz, lecz także go interpretować, wyłapywać to, co najważniejsze, i automatyzować wiele reakcji.

Dzięki temu monitoring staje się bardziej proaktywny – systemy wykrywają zdarzenia, a operatorzy skupiają się na podejmowaniu kluczowych decyzji.

Efektywność przede wszystkim

Eksperti podkreślają, że w obliczu rosnącej ilości danych zespoły bezpieczeństwa potrzebują prostych, zintegrowanych rozwiązań.

Chmura umożliwia łączenie w jednym miejscu nagrań, alarmów, kontroli dostępu i systemów antywłamaniowych, co daje pełniejszy obraz sytuacji w czasie rzeczywistym.

AI natomiast pomaga szybciej niż kiedykolwiek wyłapywać nietypowe zdarzenia i ważne wzorce w danych.

Jednocześnie rozwój chmury może zwolnić, jeśli AI nie sprawi, że stanie się ona bardziej ekonomiczna. Mimo to rozwiązania SaaS prawdopodobnie utrzymają szybki wzrost.

Rosnące znaczenie zaufanych danych

Wraz z rozwojem możliwości generatywnej AI pojawia się nowy rodzaj ryzyka: manipulowanie obrazem i danymi. Dlatego firmy coraz większy nacisk kładą na zabezpieczenie nagrań już na poziomie kamer i systemów VMS.

Coraz częściej stosuje się *blockchain*, weryfikację na brzegu sieci i niezmiennie formy przechowywania danych, które mają zagwarantować, że nagrania pozostają autentyczne.

AI pomaga dostosować systemy do rzeczywistości

Analityka AI przynosi realne korzyści – mniej fałszywych alarmów i możliwość tworzenia bardziej dopasowanych do sytuacji funkcji rozpoznawania. Nowoczesne kamery mogą być „uczone” lokalnie, by reagować na nietypowe zjawiska, a nie tylko działać według ogólnych ustawień.

Jeśli chodzi o chmurę, podejścia są różne: jedni łączą kamery bezpośrednio z chmurą, inni korzystają z bram, a jeszcze inni łączą nagrywanie na miejscu z archiwizacją online. Liczy się to, żeby rozwiązanie pasowało do budżetu i struktury firmy.

Co napędza decyzje zakupowe?

Obecnie kluczowa dla firm stała się elastyczność – możliwość szybkiego reagowania na zmieniające się wymagania i rozwijanie systemów bez zakłócania pracy. Równie ważne są integracja, możliwość pracy zdalnej, bezpieczeństwo oraz zachowanie pełnej świadomości sytuacji.

Co dalej?

Rok 2025 upływa pod znakiem trzech trendów: hybrydowej chmury, zaawansowanej analityki AI oraz rosnącego nacisku na ochronę integralności danych. Integratorzy muszą łączyć te elementy, zachowując jednocześnie zgodność, skalowalność i rozsądne koszty.

Jak zauważyli eksperci, organizacje chcą modernizować systemy w swoim tempie, stawiając na bezpieczeństwo danych i inteligentną automatyzację. Hybryda i AI stają się nowym standardem projektowania systemów bezpieczeństwa. •



Siedem kluczowych trendów monitoringu wizyjnego

Owen Kell, Memoori Research



Z

Zgodnie z najnowszymi ustaleniami Memoori Research tempo wzrostu globalnego rynku monitoringu wideo spowolniło w porównaniu z dwucyfrowymi wynikami z poprzedniej dekady. Mimo to branża ma wzrosnąć z 33,8 mld USD w 2024 r. do 47,9 mld USD w 2030 r. Ten stały rozwój maskuje jednak głębokie zmiany strukturalne – rynek przesuwają się z rozwiązań reaktywnych w stronę strategicznych inwestycji w infrastrukturę opartą na danych i analizie, gdzie wartość tworzą przede wszystkim informacje i wyniki operacyjne.

W nadchodzących latach o kształcie branży będą decydować nie tyle ulepszenia sprzętu, ile połączenie oprogramowania, uwarunkowań geopolitycznych i nowych modeli biznesowych. W oparciu o analizę rynku monitoringu wideo w latach 2025–2030 można wskazać siedem trendów, które zdefiniują konkurencyjność producentów, integratorów i użytkowników końcowych.

1. Oprogramowanie i analityka jako główne motory wzrostu

Przez lata głównym źródłem wartości w branży były sprzedaż i rozwój sprzętu. Obecnie środek ciężkości przesuwa się zdecydowanie w stronę oprogramowania i analityki. Choć cały rynek rośnie w tempie ok. 6% rocznie, segment oprogramowania do zarządzania wideo (VMS) i analityki rośnie znacznie szybciej – o 8,6%.

Oznacza to, że klienci nie kupują już tylko kamer, lecz platformy, które pozwalają przekształcić obraz w dane możliwe do analizy i wykorzystania. Udział oprogramowania w całkowitej wartości rynku ma wzrosnąć z 17% w 2024 r. do 20% w 2030 r., co sprzyja rozwojowi modeli opartych na stałych przychodach (abonamentach) i zmusza producentów sprzętu do inwestowania w oprogramowanie i ekosystemy.

2. Sztuczna inteligencja staje się standardem

Sztuczna inteligencja (AI) przestała być jedynie eksperymentem i staje się domyślnym elementem nowoczesnych systemów monitoringu. Coraz więcej kamer jest wyposażonych w funkcje uczenia maszynowego działające bezpośrednio w urządzeniu. Według analiz udział takich kamer wzrośnie z 23% w 2024 r. do 64% w 2030 r.

Rozwój ten napędzają zarówno postęp technologiczny, jak i potrzeba szybszej i dokładniejszej analizy. Użytkownicy zauważają wymierne korzyści – np. redukcję fałszywych alarmów o ponad 95%. W miarę spadku różnicy cen między kamerami z AI i bez AI inteligentne funkcje stają się nowym standardem.

3. Wielkie rozdzielenie: geopolityka zmienia rynek

Najsilniejszym czynnikiem ostatnich lat są napięcia między USA a Chinami. Amerykańskie regulacje (m.in. NDAA, FCC) stworzyły dwa równoległe rynki: jeden zdominowany przez chińskich producentów, drugi – w Ameryce Północnej i części Europy – skupiony na zgodności, przejrzystości łańcucha dostaw i cyberbezpieczeństwie.

Skutkiem jest spowolnienie wzrostu największych graczy i rozwój konkurentów zgodnych z przepisami.

Wpływ tych napięć geopolitycznych na sytuację finansową branży jest znaczący. Lider rynku, firma Hikvision, odnotowała spowolnienie rocznego wzrostu z ponad 28% w 2021 roku do zaledwie 3,5% w 2024 roku. Tymczasem producenci zgodni z wymogami NDAA, tacy jak Hanwha Vision, wykorzystali powstałą lukę na rynku, przejmując popyt ze strony sektora publicznego i infrastruktury krytycznej. Szacuje się, że ich marża EBITDA wzrośnie z 3% do 14% w 2025 roku.

Firmy muszą teraz utrzymywać zróżnicowane łańcuchy dostaw i odrębne linie produktów, co zwiększa koszty i złożoność rynku.

4. Konsolidacja rynku i rozwój platform

Na rynku przejść i fuzji dominują działania mające na celu budowę zintegrowanych platform łączących oprogramowanie, chmurę i analitykę AI. Duże firmy przejmują dostawców VMS i usług chmurowych, by oferować kompleksowe rozwiązania.

Transakcje takie, jak fuzja firmy Milestone Systems z jej spółką siostrzaną Arcules, działającą w modelu chmurowym, oraz sprzedaż działu Bosch Building Technologies przeprowadzona przez fundusze private equity, podkreślają strategiczne znaczenie tego kierunku rozwoju. Ugruntowani gracze, tacy jak Motorola Solutions czy Canon, nadal rozbudowują swoje portfele poprzez przejęcia, dążąc do objęcia kontrolą jak największej części łańcucha technologicznego – od rejestracji obrazu po jego analizę. Dla klientów oznacza to bardziej zintegrowane i wygodne rozwiązania, ale także ryzyko większego uzależnienia od jednego ekosystemu, co sprawia, że długoterminowa strategia dostawcy i jego otwartość nabierają kluczowego znaczenia.

5. Architektura hybrydowa staje się dominująca

Choć usługi monitoringu w chmurze (VSaaS) dynamicznie się rozwijają, coraz więcej organizacji stawia na model hybrydowy – łączący nagrywanie lokalne z zarządzaniem i analizą w chmurze.

Taka architektura łączy korzyści obu rozwiązań: zapewnia odporność na awarie sieci i spełnia wymagania dotyczące lokalizacji danych, a jednocześnie umożliwia centralne zarządzanie i analizę. W Europie trend ten jest szczególnie silny z uwagi na ochronę prywatności – ponad połowa firm nie planuje w 2025 r. przechowywać nagrań w chmurze.

6. Prywatność i zgodność z regulacjami – nowe wyzwania

Złożone przepisy, takie jak RODO i unijna ustawa o AI, stają się kluczowym czynnikiem kształtującym rynek. Przykładowo, stosowanie zdalnej identyfikacji biometrycznej w przestrzeni publicznej zostało praktycznie zakazane poza nielicznymi wyjątkami.

Firmy muszą wdrażać zasady *privacy-by-design* – w tym automatyczne maskowanie twarzy, kontrolę dostępu i narzędzia do anonimizacji danych. Kary finansowe za naruszenia (np. 32 mln euro dla Amazonu we Francji) pokazują, że zgodność z przepisami staje się kluczowa dla funkcjonowania na rynku.

7. Rosnące wymagania dotyczące cyberbezpieczeństwa

W miarę jak systemy monitoringu stają się coraz bardziej połączone i bogate w dane stają się również głównym celem cyberataków. Amerykański Departament Bezpieczeństwa Wewnętrznego (U.S. Department of Homeland Security) podkreśla obecnie, że systemy monitoringu wideo oparte na protokole IP należy traktować jako infrastrukturę krytyczną, wymagającą zastosowania zasad bezpieczeństwa już na etapie projektowania (*security-by-design*) na każdym poziomie. Mimo to, w połowie 2025 roku ponad 40 tysięcy urządzeń monitorujących dostępnych w sieci pozostaje publicznie widocznych i zabezpieczonych jedynie słabymi lub domyślnymi hasłami.

Ta różnica między ryzykiem a rzeczywistością szybko się zmniejsza. Użytkownicy końcowi – zwłaszcza z sektora przedsiębiorstw i administracji publicznej – coraz częściej wymagają wyższych standardów cyberbezpieczeństwa, w tym bezpiecznych procesów uruchamiania, podpisanego oprogramowania układowego oraz przejrzystych zasad zarządzania podatnościami. Regulacje, takie jak unijna dyrektywa NIS2, wprowadzają bardziej rygorystyczne obowiązki dotyczące zgłaszania naruszeń i zarządzania ryzykiem, co sprawia, że zapewnienie bezpieczeństwa cybernetycznego staje się kluczowym kryterium przy wyborze dostawców.

W miarę zbliżania się roku 2026 te trendy na nowo definiują strategiczne priorytety wszystkich uczestników łańcucha wartości w branży monitoringu. Sukces zależeć będzie nie tylko od możliwości technologicznych, lecz także od umiejętności radzenia sobie ze złożonością regulacyjną, ryzykiem geopolitycznym i rosnącymi oczekiwaniami klientów biznesowych. Coraz większe znaczenie zyska także interoperacyjność systemów oraz zdolność do szybkiego wdrażania innowacji w środowisku pełnym konkurencji. •



Rewolucja AI w security: między innowacją, inteligencją a regulacjami

Tommy Zhu, Omdia

B

Branża security przechodzi obecnie głęboką transformację wynikającą z konwergencji sztucznej inteligencji (AI), technologii chmurowych i Internetu Rzeczy (IoT). Według raportu *Omdia 2025 Video Surveillance & Analytics Report*, globalny rynek monitoringu wideo, którego wartość w 2024 r. wynosiła 25,9 mld USD, osiągnie 37,1 mld USD do 2029 r., przy średniorocznym tempie wzrostu (CAGR) na poziomie 7,5%. Rozwój ten to nie tylko postęp technologiczny – to zmiana podejścia: od tradycyjnego, reaktywnego nadzoru do proaktywnych, inteligentnych operacji bezpieczeństwa.

Cztery kluczowe trendy kształtują dziś nową rzeczywistość branży bezpieczeństwa: rozwój inteligentnych systemów AI, coraz szersze wykorzystanie przetwarzania brzegowego, zmieniające się przepisy dotyczące sztucznej inteligencji oraz rosnące znaczenie cyberbezpieczeństwa. Wszystkie te elementy są ze sobą powiązane i wzajemnie się napędzają, dlatego skuteczne działanie wymaga całościowego, dobrze skoordynowanego podejścia.

1. Generatywna i agentowa sztuczna inteligencja

Integracja generatywnej AI oraz tzw. agentowej AI zasadniczo zmienia sposób działania systemów monitoringu wizyjnego, umożliwiając przejście od reaktywnego reagowania do proaktywnego podejmowania decyzji.

Nowoczesne systemy oparte na AI wykorzystują tzw. *model vision-language* (VLM), trenowane na parach obraz-tekst, co pozwala im na znacznie bardziej zaawansowane rozumienie kontekstu niż w przypadku tradycyjnych systemów wizyjnych.

Największe modele stosowane w systemach monitoringu oferują:

- **Lepsze rozumienie kontekstu:** potrafią odróżnić podejrzané zachowanie od zwykłego oczekiwania, co znacząco ogranicza liczbę fałszywych alarmów i zwiększa skuteczność detekcji zagrożeń.
- **Szybsze wdrażanie rozwiązań:** modele bazowe umożliwiają szybkie dostosowanie do konkretnych scenariuszy i zagrożeń.



Tylko organizacje, które potrafią skutecznie połączyć inteligentne systemy AI, bezpieczną architekturę edge, zgodność regulacyjną i odporność cybernetyczną – będą w stanie w pełni wykorzystać potencjał dynamicznie rosnącego rynku.

• **Inteligencję w czasie rzeczywistym:** systemy są w stanie analizować przepływ osób i pojazdów, automatycznie wykrywać naruszenia zasad czy nietypowe wzorce zachowań, zmieniając monitoring z pasywnego nagrywania w aktywną prewencję.

2. Upowszechnienie Edge AI: architektura rozproszonej inteligencji

Wraz z rosnącą złożonością systemów AI tradycyjne, scentralizowane architektury nie są w stanie efektywnie sprostać ich wymaganiom obliczeniowym. Dlatego obserwujemy zwrot w kierunku przetwarzania brzegowego. Według analiz Omdia do 2029 r. aż 61% dostarczanych kamer będzie wyposażonych w funkcje AI.

Upowszechnienie to możliwe jest dzięki nowoczesnym technikom kompresji i optymalizacji, takim jak *knowledge distillation*, które pozwalają dużym modelom AI działać efektywnie na urządzeniach o ograniczonych zasobach. Kamery nowej generacji, wyposażone w wiele czujników i źródeł danych, zapewniają kompleksową świadomość sytuacyjną. W zastosowaniach przemysłowych potrafią współpracować np. z czujnikami wycieku gazu czy systemami wczesnego wykrywania pożarów.

W efekcie sieci bezpieczeństwa przekształcają się z prostych, centralnie zarządzanych systemów w inteligentne, autonomiczne sieci zdolne do samodzielnego podejmowania decyzji i skoordynowanej reakcji.

3. Globalne zarządzanie AI: ewolucja ram regulacyjnych

Wraz z coraz szerszym wykorzystaniem systemów zabezpieczeń opartych na sztucznej inteligencji rośnie ich znaczenie społeczne. W odpowiedzi rządy na całym świecie tworzą nowe regulacje, których celem jest zapewnienie odpowiedzialnego rozwoju i wdrażania AI, przy jednoczesnym zachowaniu przestrzeni dla innowacji.

Przełomowym momentem stało się przyjęcie unijnego **Aktu o Sztucznej Inteligencji (AI Act)** w sierpniu 2024 r., który ustanowił globalny punkt odniesienia dla zasad stosowania AI w sektorze bezpieczeństwa. Akt wprowadza jasne granice dopuszczalnych zastosowań oraz promuje odpowiedzialne innowacje.

Zgodnie z regulacjami **zabronione** są m.in.:

- **masowe pobieranie wizerunków twarzy** z nagrań CCTV,
- **rozpoznawanie emocji** w miejscach pracy i szkołach,
- **tzzw. predykcyjne profilowanie kryminalne** oparte wyłącznie na danych statystycznych.

Firmy muszą dostosować się do zmieniających się regulacji, jednocześnie zachowując sprawność operacyjną. Nowe przepisy wyznaczają standardy etycznego wykorzystania sztucznej inteligencji i ochrony danych międzynarodowych, ale niosą też ze sobą dodatkowe wyzwania – szczególnie dla rozproszonych systemów edge, które przetwarzają dane w wielu krajach jednocześnie.

4. Cyberbezpieczeństwo i prywatność: jak zarządzać paradoksem bezpieczeństwa

Choć regulacje prawne wyznaczają jasne granice odpowiedzialnego wdrażania sztucznej inteligencji, jednocześnie uwidaczniają rosnące wyzwanie – zwiększone ryzyko cyberataków wynikające z rozwoju inteligentnych i silnie połączonych systemów zabezpieczeń. Technologie, które pozwalają organizacjom przewidywać i zapobiegać zagrożeniom, mogą również otwierać nowe wektory ataku, jeśli nie zostaną odpowiednio zabezpieczone.

Nowoczesne platformy dozoru wizyjnego oparte na AI przetwarzają i gromadzą ogromne ilości wrażliwych danych i metadanych, co czyni je atrakcyjnym celem dla cyberprzestępców. Nawet pojedyncze naruszenie bezpieczeństwa może prowadzić do poważnych strat finansowych i reputacyjnych, potęgowanych przez surowe sankcje wynikające z przepisów, takich jak RODO, które przewiduje kary sięgające 4% rocznego globalnego obrotu lub 20 mln euro.

W obliczu rosnącej świadomości zagrożeń z zakresu cyberbezpieczeństwa systemów fizycznych w najbliższych latach wejdą w życie nowe regulacje – w tym unijne rozporządzenie *Cyber Resilience Act* (CRA) – nakładające obowiązek projektowania rozwiązań *secure by design* i *secure by default*. W tym kontekście skuteczne zarządzanie cyberbezpieczeństwem oraz zgodnością z przepisami staje się nie tylko wymogiem regulacyjnym, ale również kluczowym filarem zaufania i konkurencyjności w branży bezpieczeństwa.

Wnioski: konieczność zintegrowanego podejścia

Konwergencja sztucznej inteligencji, przetwarzania brzegowego, regulacji prawnych i wymogów cyberbezpieczeństwa tworzy nowy, zintegrowany ekosystem bezpieczeństwa. Łączy on ogromny potencjał rozwojowy z istotnymi wyzwaniami w zakresie zarządzania i organizacji.

Aby skutecznie funkcjonować w tym zmieniającym się otoczeniu, organizacje powinny przyjąć całościowe podejście, które obejmuje:

1. **zaawansowane rozwiązania AI** umożliwiające proaktywne wykrywanie zagrożeń z poszanowaniem regulacji,
2. **inteligencję edge** zapewniającą lokalne przetwarzanie danych i odporność na cyberataki,
3. **spójne ramy zgodności regulacyjnej** umożliwiające etyczne wdrażanie AI w różnych jurysdykcjach,
4. **kompleksowe mechanizmy ochrony danych i modeli AI** na wszystkich poziomach infrastruktury.

Tylko organizacje, które potrafią skutecznie połączyć te cztery filary transformacji – inteligentne systemy AI, bezpieczną architekturę edge, zgodność regulacyjną i odporność cybernetyczną – będą w stanie wyznaczać kierunki rozwoju inteligentnego bezpieczeństwa fizycznego i w pełni wykorzystać potencjał dynamicznie rosnącego rynku. •



Novaira Insights analizuje globalny rynek monitoringu wizyjnego

asmag.com

S

Systemy monitoringu wizyjnego pozostają kluczowym elementem ochrony ludzi, mienia i infrastruktury na całym świecie. Jak jednak wyglądała kondycja globalnego rynku w 2025 roku i jakie trendy zdefiniują jego przyszłość?

Na te pytania odpowiada **Josh Woodhouse**, główny analityk i założyciel firmy **Novaira Insights**. Ekspert podsumowuje wyniki sektora, omawia regionalne różnice oraz wskazuje technologie, które najbardziej wpływają na rozwój branży – a także kreśli prognozy na rok 2026.

Globalny rynek monitoringu wizyjnego w 2025 roku

Według danych **Novaira Insights** globalny rynek monitoringu wizyjnego wzrósł w 2025 roku o **1,7%**. Jednak wzrost ten był nierównomierny – podczas gdy **w Chinach** odnotowano spadek o **5,2%**, pozostałe regiony świata (z wyłączeniem Chin) rosły w tempie **6,1%**.

Analitycy zwracają uwagę, że 2025 rok był okresem odbicia po słabszym 2024, kiedy to rozwój hamowały wybory parlamentarne i zmiany w wydatkach publicznych w wielu krajach. W tym roku widać realizację odłożonych wcześniej inwestycji, zwłaszcza w sektorze bezpieczeństwa miejskiego i przemysłowego.

Regiony o najwyższej dynamice wzrostu

Największy potencjał wzrostu w 2025 roku wykazały rynki **Bliższego Wschodu, Ameryki Południowej, Azji Południowo-Wschodniej oraz Indii**.

Są to obszary o niższym stopniu nasycenia instalacjami monitoringu niż Ameryka Północna, Europa Zachodnia czy Chiny.

Podczas gdy w krajach rozwiniętych popyt koncentruje się głównie na **modernizacji istniejących systemów**, w gospodarkach rozwijających się obserwuje się zarówno **nowe instalacje, jak i wymianę starszego sprzętu**, co przekłada się na wyższe tempo wzrostu.

Sytuacja w Chinach

Po spadku o 7,8% w 2024 roku **rynek chiński** kontynuował trend zniżkowy również w 2025 roku.



Według analiz Novaira Insights krajowy popyt w Chinach nie wróci już do wysokich poziomów wzrostu obserwowanych w minionej dekadzie. Rynek ten osiągnął dojrzałość, a inwestycje skupiają się raczej na utrzymaniu i optymalizacji istniejących rozwiązań niż na ekspansji.

Technologie kształtujące rynek w 2025 roku

Wśród kluczowych trendów dominowały **sztuczna inteligencja (AI)** oraz rozwiązania chmurowe.

AI jest obecnie wykorzystywana głównie do zwiększania precyzji analityki wideo – od wykrywania obiektów po analizę zachowań.

Choć na rynku pojawiają się już platformy oferujące **systemową automatyzację z wykorzystaniem AI**, ich adopcja pozostaje na wczesnym etapie.

Z kolei systemy **oparte na chmurze** zyskują coraz większą popularność, zwłaszcza w Ameryce Północnej. Ułatwiają zdalne zarządzanie, skalowanie zasobów i integrację z usługami analitycznymi, co sprawia, że stają się atrakcyjną alternatywą dla tradycyjnych systemów *on-premises*.

Główne wyzwania dla branży

Rok 2025 przyniósł również szereg wyzwań, które będą towarzyszyć branży w kolejnych latach.

Do najważniejszych należą:

- bariery handlowe i cła,
- transformacja modeli biznesowych w kierunku **usług subskrypcyjnych i przychodów cyklicznych**,
- zgodność z przepisami regulacyjnymi (np. RODO, NDAA, AI Act),
- cyberbezpieczeństwo,
- niedobór wykwalifikowanych specjalistów.

Eksperti prognozują, że wszystkie te czynniki pozostaną istotnym elementem kształtującym rynek również w 2026 roku.

Prognozy i innowacje na 2026 rok

Według prognoz Novaira Insights w 2026 roku globalny rynek monitoringu wizyjnego wzrośnie o **3,1%**. Podobnie jak w poprzednim roku wzrost ten będzie napędzany przez rynki poza Chinami (wzrost o **7,4%**), podczas gdy Chiny odnotują dalszy spadek o **4,5%**.

Nowe innowacje technologiczne będą koncentrować się wokół:

- **kamer wielosensorowych** o zwiększonej wydajności i różnorodnych konfiguracjach, łączących obraz w świetle widzialnym, **radar, lidar oraz czujniki termiczne**,
- integracji **kamer z dodatkowymi czujnikami IoT**, co umożliwi pełniejsze monitorowanie środowiska i sytuacji,
- rozwoju **beprzewodowych kamer zasilanych energią słoneczną** i akumulatorami,
- wykorzystania **5G oraz zaawansowanej analityki wideo**, dzięki czemu kamery mobilne (np. tymczasowe zestawy monitoringu na przyczepach) staną się realną alternatywą dla tradycyjnych systemów zewnętrznych.

Na poziomie oprogramowania spodziewane są dalsze ulepszenia w zakresie inteligentnej **automatyzacji systemów (system-wide intelligence)**.

Platformy VMS i rozwiązania bezpieczeństwa będą coraz częściej integrować funkcje **agentowej sztucznej inteligencji (agentic AI)**, zdolnej do autonomicznego reagowania na zdarzenia i wspomagania decyzji operatorów.

Równocześnie rozwój miniaturowych modeli AI umożliwi **przetwarzanie danych na urządzeniach brzegowych (edge computing)**, co zwiększy szybkość analizy przy niższym zużyciu energii i kosztach operacyjnych.

Podsumowanie

Rok 2025 był dla globalnego rynku monitoringu wizyjnego okresem stabilizacji po latach zawirowań gospodarczych i geopolitycznych. Jednocześnie stał się punktem wyjścia do kolejnej fazy transformacji – opartej na sztucznej inteligencji, analizie danych i integracji systemów bezpieczeństwa z chmurą i IoT.

Patrząc w przyszłość, branża zmierza w kierunku **inteligentnych, zrównoważonych i połączonych ekosystemów bezpieczeństwa**, w których monitoring wideo stanie się centralnym elementem nie tylko ochrony, ale i zarządzania środowiskiem operacyjnym organizacji. •



Jak **wideoanalityka** pomaga zrozumieć zachowania kupujących w sklepach



Współczesny handel detaliczny coraz częściej opiera się na danych. W e-commerce zbieranie informacji o zachowaniu użytkowników jest standardem – retailerzy online znają ścieżki zakupowe klientów, mierzą współczynniki konwersji, badają skuteczność kampanii oraz analizują elementy wpływające na tzw. *user experience*. Tymczasem w sklepach stacjonarnych podobne wskaźniki wciąż nie są wykorzystywane w takim stopniu, w jakim mogłyby być. Brakuje nie tylko doświadczenia w analizie danych, ale i świadomości, że wiele informacji można dziś pozyskać szybko, tanio i bez złożonych systemów opartych o kosztowne algorytmy AI.

W praktyce często pomijane są narzędzia, które od lat są obecne na rynku i które – przy właściwym wdrożeniu – pozwalają realnie podnieść efektywność funkcjonowania sklepu. Mowa przede wszystkim o nowoczesnej wideoanalizie, coraz częściej integrującej funkcje AIoT oraz klasyczne rozwiązania CCTV. Dzięki niej retailerzy mogą wreszcie zbudować pełny obraz zachowań klientów i przełożyć te dane na decyzje operacyjne, marketingowe oraz sprzedażowe.

Liczniki odwiedzin – fundament analityki w retailu

W wielu sklepach liczba wydawanych paragonów pełni funkcję jedyne miernika wizyty klienta. W przypadku dyskontów czy supermarketów takie podejście bywa wystarczające, bo odsetek osób wychodzących bez zakupu jest minimalny. Jednak w branżach takich jak fashion, elektronika czy DIY sytuacja wygląda zupełnie inaczej. Klienci często odwiedzają sklep, ale nie znajdują odpowiedniego modelu, koloru, rozmiaru lub funkcjonalności produktu.

Dlatego kluczowe jest poznanie realnej liczby odwiedzających, a nie tylko kupujących. Porównanie liczby wejść z liczbą transakcji pozwala na obliczenie współczynnika konwersji i zadanie właściwych pytań:

- czy w sklepie brakuje odpowiednich produktów?
- czy oferta jest właściwie zaprezentowana?
- czy klient potrafi znaleźć to, czego szuka?

W tym obszarze świetnie sprawdzają się oferowane przez Hikvision kamery z funkcją **people counting**, takie jak **Hikvision iDS-2CD7146G2-IZ(H)S(Y)(1T)**. Warto tu

wspomnieć o funkcji **pass-by**, pozwalającej na określenie liczby osób przechodzących obok sklepu. Dla punktów zlokalizowanych w galeriach handlowych to narzędzie, dzięki któremu można ocenić potencjalny ruch i zestawzić go z faktyczną liczbą odwiedzin.

Czas przebywania w sklepie – wskaźnik zaangażowania

Wideoanalityka umożliwia również mierzenie czasu, jaki klienci spędzają w sklepie. To szczególnie wartościowy parametr, gdy zestaw się go z licznikiem wejść, porą dnia, sezonowością czy danymi z systemu POS. Dłuższy czas przebywania może świadczyć o wysokim zainteresowaniu ofertą, ale też o problemach z nawigacją po sklepie.

Heatmapy – najcenniejsze narzędzie shoppa

W kontekście handlu detalicznego heatmapy są jedną z najbardziej wartościowych funkcjonalności. Pokazują rzeczywiste ścieżki poruszania się klientów, ich koncentrację w różnych strefach oraz miejsca ignorowane. Umożliwiają również ocenę skuteczności



ekspozycji, promocji oraz zmian w layoucie sklepu. Tu warto zapoznać się z kamerą **DS-2CD63C5G1-IVS**.

Pełna analiza sprzedaży dzięki korelacji danych

Gdy dysponujemy już liczbą klientów, ich ścieżkami, czasem przebywania w sklepie i danymi o punktach koncentracji ruchu – zaczyna się właściwa analiza sprzedażowa. Połączenie systemów CCTV z POS-em pozwala na zrozumienie, które produkty przyciągają uwagę, jak wygląda interakcja klientów z konkretnymi regałami i jak zachowania zakupowe przekładają się na wyniki finansowe sklepu.

Tego typu integracje to dziś standard, a Hikvision od lat oferuje gotowe narzędzia umożliwiające łączenie nagrań z danymi transakcyjnymi, co pozwala również wykrywać nieprawidłowości i minimalizować straty.

Triggerowanie – operacje sklepu w czasie rzeczywistym

Jedną z najbardziej praktycznych funkcji wideoanalitiky jest możliwość automatycznego

wywoływania akcji w odpowiedzi na zachowania klientów. Przykładów jest wiele:

- automatyczne uruchamianie kolejnych kas po przekroczeniu limitu osób w kolejce,
- wysyłanie kasjera mobilnego na stację paliw, gdy tworzą się zatory przy dystrybutorach,
- emisja komunikatów audio kierujących klientów do kas samoobsługowych,
- dynamiczna zmiana kontentu Digital Signage w zależności od profilu ruchu,
- regulacja muzyki tła zależnie od natężenia wizyt.

Przyszłość retailu jest oparta na danych – i dostępna już dziś

Wbrew pozorom stworzenie kompleksowego systemu analitiky wideo nie wymaga ogromnych inwestycji. Dzisiejsze rozwiązania AIoT oraz kamery z funkcjami inteligentnej detekcji są przystępne cenowo i skalowalne, a ich wdrożenie nie wymaga rewolucji technologicznej.

Wystarczy zdefiniować, jakie dane są potrzebne, w jaki sposób będą wyko-

rzystywane oraz jak mają wspierać codzienne procesy. Retail od lat ewoluuje, a technologia – choć dostępna – nie zawsze jest wykorzystywana w pełni. Tymczasem to właśnie wideoanalitika może stać się tym elementem, który na nowo zdefiniuje sposób funkcjonowania sklepów, pozwalając im działać bardziej efektywnie, precyzyjnie i w oparciu o rzetelne dane.

Rozwiązania Hikvision pokazują, że zaawansowana analitika nie musi oznaczać kosztownych wdrożeń. Wystarczy rozsądnie dobrany zestaw kamer i odpowiednia konfiguracja, aby znacząco zwiększyć sprzedaż, poprawić jakość obsługi i zoptymalizować procesy operacyjne. A to właśnie w dzisiejszym handlu stacjonarnym jest najcenniejszą przewagą konkurencyjną. •



Hikvision Poland

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



Rosnące straty w handlu – problem, który wymaga reakcji

Mimo że 92% sklepów monitoruje kradzieże zewnętrzne, straty nadal rosną. Najnowsze badanie SGH i **Checkpoint Systems** pokazuje, że w 23% firm poziom strat nieznanych wzrósł, co oznacza, że obecnie najczęściej wykorzystywane zabezpieczenia są niewystarczające.

Aż 83,2% kradzieży ma charakter przypadkowy, wynikający z impulsu lub nieuwagi personelu. Najczęstsze metody kradzieży obejmują: chowanie produktów do toreb i plecaków (77%), korzystanie z nieuwagi obsługi (15%), zrywanie zabezpieczeń (12%) oraz konsumpcję w sklepie (8%). To zachowania trudne do kontrolowania bez odpowiednich technologii.

Badanie ujawnia istotną lukę inwestycyjną. Najpopularniejszym rozwiązaniem pozostaje monitoring CCTV, stosowany przez 85,8% sklepów, mimo że jego skuteczność oceniono jedynie na 59,8%. Z kolei bramki EAS, uznawane za znacznie skuteczniejsze (83,6%), stosowane są rzadziej – tylko w 57,7% placówek. Najbardziej efektywne okazują się systemy RFID (skuteczność aż 90%), ale wykorzystuje je zaledwie 5,1% sklepów.

Wzrost kradzieżowości i niska efektywność najczęściej wybieranych rozwiązań pokazują, że handel musi zacząć inwestować bardziej świadomie – w technologie, które odpowiadają na rzeczywiste zagrożenia.

Jednym z takich rozwiązań jest nowoczesna platforma **SFERO™** firmy Checkpoint Systems oparta na technologii RFID, która łączy detekcję kradzionych towarów z możliwością

inwentaryzacji produktów. System oferuje bardzo wysoką skuteczność (ponad 95% detekcji) i elastyczność dopasowania do układu sklepu. Anteny mogą być montowane jako klasyczne bramki przy wejściu, ale też pod sufitem lub w nietypowych miejscach. Dzięki temu nawet przy próbach kradzieży w torbie/plecaku, system ma dużą szansę wykrycia nieautoryzowanego wyniesienia towaru.

Kolejne rozwiązanie tego światowego lidera rozwiązań dla handlu detalicznego to klasyczne bramki antykradzieżowe **EAS RF**, które nadal stanowią skuteczną pierwszą linię obrony. Systemy EAS zapewniają wykrywanie tagów RF przy próbie opuszczenia sklepu. Taki rodzaj zabezpieczeń redukuje ryzyko kradzieży w momentach nieuwagi personelu lub przy próbach wyjścia z towarem bez zapłaty.

Niektórzy złodzieje próbują ominąć systemy EAS, chowając towar w specjalnych torbach lub używając metalowych wózków, by stłumić sygnał. W takich sytuacjach najlepiej sprawdzą się rozwiązania detekcji metali, takie jak **Hyperguard™** i **Metalguard™** marki **Checkpoint**. Wykrywają one próby obejścia zabezpieczeń i generują dyskretne alarmy dla personelu sklepu. To ważny element ochrony przed bardziej zorganizowaną kradzieżą.

Dodatkową warstwą ochrony mogą być **etykiety SWAT**. W momencie próby usunięcia takiej etykiety zostawia ona permanentny znak na produkcie, co utrudnia późniejszą odsprzedaż skradzionego towaru. To rozwiązanie „odstrasżające”, bo zmniejsza potencjalny zysk złodziei. W sklepach, gdzie większość kradzieży to przypadkowe działania, taka bariera psychologiczna bywa bardzo skuteczna.

Biorąc pod uwagę metody kradzieży, najbardziej sensownym rozwiązaniem jest stosowanie różnych technologii ochrony jednocześnie. Niezależna instalacja systemów zabezpieczających Checkpoint Systems czy też połączenie popularnego monitoringu CCTV wraz z bramkami EAS, detekcją metali i etykietami daje realną szansę na znaczącą redukcję strat, zwiększenie bezpieczeństwa pracowników oraz ochronę marży i wzrost rentowności. •



Checkpoint Systems Polska
ul. L. Idzikowskiego 16
00-710 Warszawa
biuro@checkpoint.com



Polskie profesjonalne
zintegrowane rozwiązania
VMS

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



www.alnetsystems.com



Głos branży



Dynamiczny rozwój handlu sprawia, że kwestie bezpieczeństwa w sklepach nabierają kluczowego znaczenia. Eksperci podkreślają, że skuteczna ochrona przed kradzieżami, zapobieganie stratom i właściwa organizacja zabezpieczeń są ważniejsze niż sam potencjał zastosowanych technologii. Coraz większą rolę odgrywają też rozwiązania systemowe, w tym sygnalizacja pożarowa na parkingach. Prezentujemy opinie specjalistów na temat realnej skuteczności współczesnych metod zabezpieczania mienia.

Ochrona przed kradzieżami w sklepach

WOJCIECH KAWA
EKSPERT DS. ZABEZPIECZEŃ



Kradzieże w handlu detalicznym były, są i będą. Niezależnie od tego, czy wynikają z trudnej sytuacji ekonomicznej, wysokiej inflacji, czy zwykłej chęci szybkiego zysku, straty zawsze ponosi sprzedawca. Wciąż jednak wiele firm traktuje pewien poziom strat jako naturalny element działalności, co prowadzi do braku determinacji w budowaniu skutecznych systemów bezpieczeństwa.

Takie ciche przyzwolenie wzmacnia zuchwałość nieuczciwych konsumentów, którzy często doskonale wiedzą, gdzie znajdują się atrapy urządzeń zabezpieczających, w których sklepach brakuje obsługi, a gdzie nadzór jest symboliczny. Część placówek stosuje jedynie minimalne zabezpieczenia, np. oznacza klipsami tylko najdroższe butelki alkoholu lub montuje imitacje kamer czy bramek, uzupełniając je jedynie tabliczkami informującymi o rzekomym pełnym monitoringu. Są to działania pozorne i niespójne, które nie tworzą realnego systemu ochrony.

Źródłem problemu jest często przypadkowość w budowaniu zabezpieczeń. W jednym sklepie funkcjonują systemy od różnych dostawców, które nie współpracują ze sobą i ograniczają możliwość wdrażania nowoczesnych rozwiązań. Nierzadko sklep opiera się wyłącznie na monitoringu wizyjnym i pracy ochrony, co nie jest wystarczające.

Zupełnie inaczej wygląda sytuacja w modelu franczyzowym. Ujednolicony projekt sklepów, podobne metraże oraz identyczny asortyment sprawiają, że rozwiązania antykradzieżowe są łatwiejsze do standaryzacji, bardziej opłacalne i szybkie do wdrożenia na szeroką skalę.

W przypadku małych sklepów barierą pozostaje niska rentowność, często nieprzekraczająca 1 proc. Przy tak niewielkich marżach trudno wygospodarować środki na zaawansowane systemy zabezpieczeń, co zmusza właścicieli do ograniczania się do najtańszych form ochrony.

Dobór metod zabezpieczenia powinien zależeć od formatu sklepu oraz dostępnych zasobów finansowych. W hipermarketach spotyka się rozbudowane modele ochrony łączące środki organizacyjne, personalne i infrastrukturalne: monitoring wizyjny, kontrolę dostępu, bramki antykradzieżowe, systemy kasek, ochronę fizyczną, detektywyw sklepowych oraz szczegółowe procedury. Natomiast sklepy typu *convenience* zwykle opierają się głównie na kamerach, systemach sygnalizujących wejście klienta oraz wsparciu mobilnych patroli ochrony.

Choć człowiek jest najsłabszym ogniwem systemu, nie należy zapominać, że technologia nie zawsze zastępuje pracownika, częściej go uzupełnia, tworząc bardziej skuteczne, zintegrowane rozwiązania. Kluczową rolę nadal odgrywa dobrze przeszkolony i zmotywowany personel ochrony, wspierany przez nowoczesne narzędzia, takie jak inteligentna analityka obrazu czy współpraca z centrum monitoringu.

Podsumowując, skuteczna ochrona obiektów handlowych to złożony proces, wymagający rzetelnej analizy, przemyślanego doboru środków bezpieczeństwa oraz wdrażania dobrych praktyk. Stałe monitorowanie zagrożeń i rozwijanie stosowanych rozwiązań są niezbędne, by realnie ograniczać straty wynikające z kradzieży. Jednym z najsukuteczniejszych elementów takiego systemu pozostają bramki antykradzieżowe i profesjonalne akcesoria zabezpieczające.

Zapobieganie stratom

JAROSŁAW KOZIEŁ
EMPIK



Handel od zawsze był narażony na straty, choć przyczyny i mechanizmy ich powstawania zmieniały się wraz z rozwojem technologii i gospodarki. Obecnie tradycyjne systemy zabezpieczeń w handlu detalicznym mierzą się z coraz większymi trudnościami w skutecznym przeciwdziałaniu kradzieżom.

Zatowarowanie sklepów, rosnące oczekiwania klientów, a także procesy związane z planowaniem, organizacją i zarządzaniem zasobami wyznaczają kierunek w ekspozycji produktów szczególnie narażonych na kradzież. Produkty te muszą być w pełni dostępne dla klienta, a sposób ich zabezpieczenia nie może utrudniać dostępu do informacji ani zakupu.

Do dyspozycji pozostaje szeroka gama zabezpieczeń antykradzieżowych dopasowanych do rozmiaru, wartości i atrakcyjności towaru, m.in. klipsy z alarmem, safery, a także zabezpieczenia AM, EM i RF (stickery imitujące kody kreskowe, metki VAS, klipsy). W połączeniu z odpowiednio dobranymi systemami antykradzieżowymi oraz monitoringiem CCTV tworzą one skuteczną barierę ochronną.

Warto jednak pamiętać, że nawet najlepszy system nie zadziała bez właściwie przeszkolonych pracowników, przejrzystych struktur oraz jasno określonych zadań, ukierunkowanych na realizację konkretnych celów.

Istotnym elementem jest również opracowanie indywidualnych planów inwentaryzacyjnych dla salonów oraz wdrożenie pakietów działań, takich jak inwentaryzacje wybranych kategorii, codzienna ewidencja produktów wrażliwych, szybki przepływ informacji i niezwłoczna weryfikacja braków na stanie połączona z odpowiednią reakcją personelu. Pozwala to tworzyć dopasowane do danego salonu schematy ochrony przed kradzieżą.

Zadaniem menedżerów ds. zapobiegania stratom jest nieustanne aktualizowanie taktyk prewencyjnych oraz wypracowywanie nowych, skuteczniejszych metod przeciwdziałania kradzieżom, wykraczających poza standardowe rozwiązania. To właśnie działania operacyjne, realizowane na co dzień przez wykwalifikowany zespół *loss prevention*, stanowią fundament efektywnego systemu bezpieczeństwa.

Warto pamiętać, że kradzież sklepowa nie kończy się na samym zaborze mienia – skradzione produkty muszą zostać gdzieś sprzedane. Kluczem do skutecznego przeciwdziałania jest identyfikacja potencjalnych punktów skupu oraz analiza rynku pod kątem zjawiska paserstwa. Otwiera to drogę do szeregu działań operacyjnych połączonych ze ścisłą współpracą z organami ścigania.

Bezpieczeństwo w handlu

ROBERT KUJAWA
RETAIL SECURITY ACADEMY



Poziom zabezpieczeń w polskim handlu oceniam jako zadowalającą, choć wciąż bardzo nierówną. Wyraźny postęp widać przede wszystkim w dużych sieciach, zwłaszcza po 2023 r., kiedy odnotowano rekordowe wskaźniki kradzieży. Rośnie wykorzystanie analityki wideo, nowej generacji systemów EAS oraz standardów CPTED w aranżacji sklepów. Coraz częściej pojawia się też podejście holistyczne: audyty, mapowanie ryzyk, praca na wskaźnikach oraz bliższa współpraca między działami.

W mniejszych placówkach nadal obserwuję jednak znaczące rozbieżności. Spotyka się zarówno dobrze skonfigurowane rozwiązania, jak i obiekty, w których monitoring pełni jedynie funkcję „odstraszacza”, a inne systemy nie są stosowane. Procedury bywają nieegzekwowane lub nie istnieją, co generuje największą część strat. Brakuje szkoleń pracowników, a podstawowe przepisy dotyczące m.in. kradzieży, kradzieży zuchwałej, czynu ciągłego, oszustwa czy kradzieży pracowniczych są często nieznanne. W efekcie nawet zatrzymanie sprawcy często kończy się jedynie mandatem, a reakcje personelu wynikają z emocji, a nie z procedur. To, że statystyki policji wskazują na niższą liczbę kradzieży w małych sklepach, nie oznacza, że jest ich

tam mniej – wiele placówek rezygnuje ze zgłaszania z uwagi na czasochłonne procedury.

Czy inwestować w systemy techniczne, czy w ochronę fizyczną? W branży retail to nie jest wybór „albo-albo”. Najskuteczniejszy model opiera się na integracji technologii, procedur i dobrze przygotowanego personelu. Jeśli jednak miałbym wskazać obszar o najwyższej stopie zwrotu, byłyby to systemy techniczne: inteligentny monitoring, zaawansowane EAS, kontrola operacyjna POS i analityka danych. Technologia działa 24/7, ogranicza błędy ludzkie i pozwala wcześniej wykrywać nadużycia. Ochrona fizyczna pozostaje kluczowa tam, gdzie występuje ryzyko agresji, nasilonych kradzieży, aktywności grup zorganizowanych lub specyfika obiektu wymaga natychmiastowej reakcji. Jest jednak skuteczna tylko wtedy, gdy w placówkach pracują odpowiednio przeszkoleni specjaliści, a nie przypadkowe osoby. Ochrona powinna działać w ścisłej współpracy z personelem sklepu, opierając się na realnych danych i właściwie skonfigurowanych systemach.

Podsumowując, przyszłość bezpieczeństwa to nie wybór między człowiekiem a technologią, lecz budowanie spójnych, mierzalnych procesów, w których oba elementy wzajemnie się wzmacniają.



Sam potencjał nie chroni mienia

ADAM SULIGA
SAFETY PROJECT



W ostatnich miesiącach w branży retail obserwujemy niemal bezkrytyczny entuzjazm wobec nowych technologii zabezpieczających: systemów CCTV wspieranych przez AI, rozwiązań RFID czy zaawansowanych platform analitycznych. Owszem, te rozwiązania mają ogromny potencjał, ponieważ szybciej niż człowiek i z dużo większą dokładnością potrafią wykrywać anomalie, automatyzować procesy i generować dane wspierające proces zarządzania stratami. Mogą nawet stanowić punkt wyjścia do przygotowania działań prewencyjnych i profilaktycznych. Problem w tym, że sam potencjał nie chroni mienia. Technologia jest jedynie narzędziem, a nie zastępstwem dla profesjonalnej ochrony.

W praktyce bowiem nadal kluczowym elementem Skutecznego Systemu Bezpieczeństwa jest człowiek – odpowiednio

wyselekcjonowany, przeszkolony i świadomy postawionych przed nim zadań. Tymczasem wielu zarządców obiektów handlowych ulega iluzji, że inwestycja w „inteligentne” rozwiązania może zrekompensować braki kadrowe lub obniżyć koszty personalne. To błędne założenie. Nawet najbardziej zaawansowana analityka obrazu nie przyniesie efektu, jeśli operator nie potrafi właściwie interpretować alarmów ani szybko reagować. RFID nie ograniczy strat, jeśli pracownik nie rozumie, jak funkcjonują procesy logistyczne i gdzie najczęściej pojawiają się luki. W tym względzie profesjonalizacja służb ochrony to wymóg. To obowiązek zarówno organizacji branżowych, jak i ustawodawcy, który wciąż biernie przygląda się postępującemu kryzysowi tego środowiska.

Bez profesjonalnej ochrony technologia staje się jedynie droгим gadżetem. W efekcie firmy ponoszą koszty zakupu, wdrożenia i utrzymania systemów, które nie przekładają się na realne zmniejszenie liczby niepożądanych incydentów oraz nie poprawiają skuteczności ich wykrywania. Klucz do efektywności leży w synergii: odpowiednie narzędzia plus właściwie przygotowany personel. Dopiero wtedy inwestycje w nowe technologie przestają być wydatkiem, a zaczynają być realnym wsparciem operacyjnym.

Realna skuteczność zabezpieczeń

MIROSLAW ŁUKOWSKI
EKSPERT DS. BEZPIECZEŃSTWA



Jak dziś można ocenić poziom zabezpieczenia placówek handlowych przed kradzieżami? Wszystko zależy od przyjętych założeń oraz statystyk wykrywalności. Jeżeli rozpatrujemy kradzież zewnętrzną, należy zadać pytanie: czy istnieją rozwiązania, które w 100% zabezpieczają obiekt? Wszyscy doświadczeni menedżerowie bezpieczeństwa wiedzą, że takich zabezpieczeń nie ma. W dobie optymalizacji zatrudnienia, powszechnych kas samoobsługowych oraz nieustannej walki o wynik finansowy uważam, że poziom zabezpieczenia drastycznie maleje.

Wprowadzanie każdej nowej technologii ułatwiającej zakupy, zarówno kas samoobsługowych, jak i aplikacji mobilnych, wymusza na sieciach handlowych rezygnację ze starych, mechanicznych sposobów zabezpieczania produktów wrażliwych. Prowadzi to niestety do zmniejszenia liczby zabezpieczanych PLU (*Price Look-Up* – numerycznego kodu używanego w handlu do identyfikacji i wyceny produktów, zwłaszcza tych sprzedawanych na wagę lub pozbawionych kodów kreskowych, jak owoce czy warzywa).

Dziś osoby działające na szkodę sieci handlowych dysponują technikami umożliwiającymi zakłócanie pracy systemów antykradzieżowych. Rozwiązania powszechnie dostępne na portalach zakupowych ułatwiają ten przestępczy proceder. Jeszcze kilka lat temu stoiska alkoholowe były wydzielone, posiadały obsługę i osobne stanowiska kasowe. Dziś kasy samoobsługowe wymagają jedynie potwierdzenia wieku, które często odbywa się zdalnie z kasy liniowej, bez weryfikacji dokumentu tożsamości.

Automatyzacja stworzyła szerokie pole do kreatywnych działań przestępczych.

Oddzielnym problemem są kradzieże wewnętrzne. Tu doświadczenie podpowiada, że tylko odpowiednie procedury oparte na głębokiej analizie procesów oraz konsekwentne ich przestrzeganie pozwalają ograniczyć straty, a nawet skutecznie je zatrzymać.

Otwarte pozostaje pytanie: czy kradzież to jedyna i najważniejsza strata sklepu? Przez lata pracy w handlu zdobyłem doświadczenie, które pozwala mi sądzić, że NIE. Niegospodarność, brak umiejętnego zarządzania zapasem, brak kontroli zamówień i dostaw oraz niewłaściwa analiza strat znanych generują straty, które często w raportach automatycznie zaliczane są do strat nieznanego, zniekształcając statystyki kradzieży.

Każdy dzień pracy w tak dynamicznym sektorze, jak handel detaliczny, uczy. Moje doświadczenie pokazuje, że połączenie zaawansowanej technologii z dobrze wyszkolonym zespołem pracowników ochrony daje najlepszy efekt w walce ze stratą zarówno znaną, jak i nieznaną.

Niestety sytuacja w branży ochrony sprzyja oferowaniu sieciom handlowym usług opartych na przypadkowo zatrudnianych pracownikach, którzy dopiero na obiektach uczą się zawodu. To obciąża menedżerów ochrony odpowiedzialnych za placówki, wymaga inwestycji oraz czasu, a często skutkuje rotacją i koniecznością ciągłego rozpoczynania procesu szkoleniowego od nowa.

Technologia pozwala skupić się na kluczowych, wrażliwych strefach działania placówki handlowej, a w pełni wykorzystana daje ogromne wsparcie w walce z kradzieżami. To jednak jedynie narzędzie. Po drugiej stronie musi być człowiek, który potrafi wykorzystać je w 100%.

Technologia czy człowiek? Moim zdaniem tylko odpowiednia proporcja obu tych elementów może przynieść realny efekt. Niestety w praktyce często jeden z nich znacząco odstaje od drugiego.



Sygnalizacja pożarowa na parkingach

MARCIN WALCZUK
BCS



Galerie handlowe to złożone obiekty, w których obok przestrzeni zakupowych funkcjonują również rozbudowane parkingi, często podziemne lub wielopoziomowe. To właśnie one stawiają szczególne wyzwania w zakresie ochrony przeciwpożarowej. W takich miejscach systemy sygnalizacji pożarowej odgrywają kluczową rolę, zapewniając wczesne wykrycie zagrożenia i umożliwiając sprawne przeprowadzenie działań ratowniczych. Dlatego stosuje się specjalistyczne systemy sygnalizacji pożarowej, których zadaniem jest szybkie wykrycie zagrożenia, uruchomienie alarmu oraz wsparcie działań ewakuacyjnych i gaśniczych.

Podstawową funkcją systemu jest wczesne wykrywanie pożaru lub zapobieganie jego powstaniu. W tym celu stosuje się różne typy urządzeń reagujących na obecność dymu lub gazów powstających w procesie spalania. Na parkingach szczególnie istotne są czujniki odporne na zakłócenia wynikające z obecności spalin samochodowych, mogących powodować fałszywe alarmy. Oprócz klasycznych czujników dymu wykorzystuje się czujniki temperatury, reagujące na gwałtowny wzrost ciepła, oraz czujniki gazów monitorujące stężenie tlenku węgla i innych toksycznych substancji. Ciekawym rozwiązaniem są kamery termowizyjne, takie jak model BCS-L-EIP54IFSR2-EDT, wykrywające pożar lub monitorujące poziom temperatury. Przekroczenie określonego progu temperaturowego skutkuje uruchomieniem alarmu.

System sygnalizacji pożarowej nie ogranicza się jedynie do wykrywania pożaru. Jego zadaniem jest także alarmowanie

użytkowników poprzez sygnały akustyczne i optyczne oraz sterowanie innymi urządzeniami przeciwpożarowymi. W przypadku wykrycia zagrożenia system może automatycznie uruchomić wentylację oddymiającą, zamknąć kłapy przeciwpożarowe czy aktywować instalacje tryskaczowe. Szczególnie istotna jest integracja z systemem wentylacji, który w momencie pożaru usuwa dym i gorące gazy, kieruje przepływem powietrza tak, aby ułatwić ewakuację i ograniczyć rozprzestrzenianie się toksycznych substancji.

Projektowanie systemów sygnalizacji pożarowej na parkingach wiąże się z licznymi wyzwaniami. Należy uwzględnić możliwość zakłóceń powodowanych przez spaliny, duże przestrzenie wymagające odpowiedniego rozmieszczenia czujników oraz trudne warunki środowiskowe, takie jak wilgoć czy kurz. Systemy muszą być odporne na te czynniki, aby działały niezawodnie. Coraz częściej integruje się je również z monitoringiem wizyjnym, co pozwala na szybszą ocenę sytuacji i podjęcie odpowiednich działań przez służby ratownicze.

Znaczenie systemów sygnalizacji pożarowej na parkingach jest ogromne. Chronią one życie i zdrowie użytkowników, minimalizują straty materialne, wspierają działania straży pożarnej i zwiększają poczucie bezpieczeństwa w przestrzeni publicznej. W nowoczesnych miastach stają się standardem, a ich rozwój idzie w parze z rosnącą liczbą pojazdów i potrzebą zapewnienia bezpiecznej infrastruktury. Dzięki nim możliwe jest szybkie reagowanie na zagrożenia, co w przypadku pożaru ma kluczowe znaczenie dla skuteczności akcji ratowniczej i ograniczenia skutków zdarzenia.



Mobilne wieże do monitoringu nie tylko na placach budowy

ARTUR NOWAKOWSKI
LINC POLSKA



Niedawne wysadzenie fragmentu torów kolejowych pokazało, jak realne i nieprzewidywalne stały się zagrożenia o charakterze sabotażowym. Incydent ten unaoczniał, że działania destrukcyjne mogą pojawić się nagle i w miejscach, które wcześniej uznawano za bezpieczne. W takich sytuacjach szczególnie wartościowe stają się rozwiązania służące do natychmiastowego wzmocnienia ochrony, które można wdrożyć w ciągu godzin, a nie tygodni. Jednym z takich rozwiązań są mobilne wieże do monitoringu, które pozwalają reagować skutecznie i elastycznie.

Mobilne wieże możemy zaliczyć do najszybciej rosnących trendów w branży zabezpieczeń technicznych. Kojarzone głównie z placami budowy, dziś coraz częściej stanowią optymalną odpowiedź na potrzebę skutecznego zabezpieczania parkingów, centrów logistycznych, magazynów zewnętrznych czy placów składowych. Ich popularność wynika z praktycznej konstrukcji, która łączy w jeden wielofunkcyjny system uzupełniające się urządzenia: kamery dzień i noc, termowizyjny, zaawansowaną analitykę obrazu, łączność komórkową oraz niezależne źródła zasilania.

Kluczową przewagą mobilnych wież jest możliwość natychmiastowego uruchomienia monitoringu w dowolnym miejscu, bez budowy infrastruktury, wykopów czy prowadzenia kabli. Taka wieża może zostać rozstawiona i uruchomiona nawet w kilkanaście minut po przywiezieniu na teren obiektu. Rozwiązanie to sprawdzi się wszędzie tam, gdzie pojawia się potrzeba szybkiej reakcji na zwiększone ryzyko kradzieży, wandalizmu lub wtargnięcia osób nieuprawnionych.

Niezależnie od tego, czy mówimy o infrastrukturze liniowej, czy o obiektach punktowych, jak stacje energetyczne, ujęcia wody lub przemysłowe składy materiałów, wieże do monitoringu pozwalają szybko i skutecznie zabezpieczyć wybrany obszar. Taka elastyczność jest bardzo cenna, gdy pojawia się konieczność reakcji na działania o charakterze nagłym i destabilizacyjnym.

Mobilne wieże mogą również pełnić funkcję w ochronie obszarów przygranicznych w miejscach wymagających pilnego zwiększenia nadzoru, np. jako wsparcie w procesie wykrywania prób przemytu towarów lub nielegalnego przekroczenia granicy. Z uwagi na niezależne zasilanie, analitykę wideo oraz możliwość pracy w trudnych warunkach terenowych wieże sprawdzają się jako narzędzie czasowego wsparcia służb.

Coraz większą rolę odgrywa również wykorzystanie mobilnych wież w systemach antydronowych. Wyposażone w radary krótkiego zasięgu i detektory sygnałów radiowych mogą być stosowane jako mobilne punkty wykrywania dronów używanych do przemytu, obserwacji czy działań sabotażowych. W połączeniu z kamerami obserwacyjnymi pozwalają na wczesne wykrycie zagrożenia i szybką reakcję.

W świecie, w którym poziom ryzyka zmienia się z dnia na dzień, mobilne wieże do monitoringu oferują unikalną możliwość natychmiastowego podniesienia poziomu bezpieczeństwa. Przede wszystkim pozwalają szybko i skutecznie zabezpieczyć obiekty narażone na kradzieże, akty wandalizmu, nielegalne wtargnięcia oraz inne działania destrukcyjne.

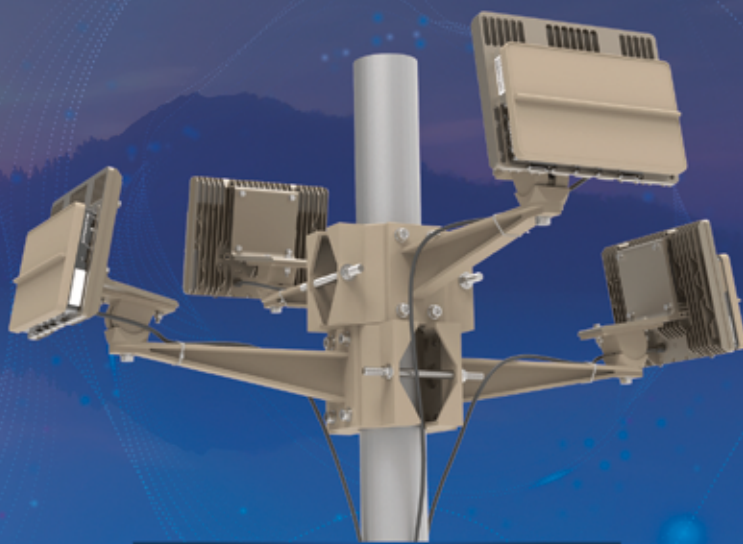


ECHODYNE



EchoShield®

WIELOZADANIOWY RADAR 4D



EchoGuard®

KOMPAKTOWY RADAR 4D

POLE WIDZENIA

do 130° w poziomie
do 90° w pionie

IDENTYFIKACJA I ŚLEDZENIE

do 40 obiektów o wysokim oraz
do 1000 obiektów o niskim
priorytecie

SKUTECZNOŚĆ

identyfikacja dronów
do 100%

SYGNATURA μDOPPLER

klasyfikacja dronów,
rozróżnienie od innych obiektów
jak ptaki czy ludzie



1.5 km

2.7 km

4.8 km

6.4 km

11 km

30 km

250 m

1 km

1.4 km

2.2 km

3.5 km

6 km

OFICJALNY DYSTRYBUTOR:

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

www.linc.pl

WIĘCEJ O NAS:



Linc
Polska Sp. z o.o.

Lekcja z Luwru: jak naprawdę powinny działać zabezpieczenia muzeów?

Zuchwała kradzież, do której doszło niedawno w Luwrze, ponownie uruchomiła dyskusję na temat bezpieczeństwa muzeów i ochrony bezcennych zbiorów. O tym, jakie wnioski płyną z tego incydentu dla polskich instytucji kultury, jak powinny wyglądać skuteczne procedury oraz dlaczego technologia nigdy nie zastąpi czujności człowieka, rozmawiamy z **Arturem Boguszem** – kierownikiem działu bezpieczeństwa Muzeum Historii Polski.



Ma Pan bogate doświadczenie w zabezpieczaniu obiektów, w tym muzeów. Z tej perspektywy, jakie refleksje nasunęły się Panu po kradzieży w Luwrze?

Pierwsze, co zwróciło moją uwagę, to nieskuteczność działania. Mówiąc wprost: co z tego, że są określone zabezpieczenia, istnieje ochrona fizyczna i procedury, skoro brakuje ich testowania i ćwiczenia. Kiedy więc dochodzi do niepożądanego zdarzenia, reakcja jest opóźniona albo niewłaściwa – i tak właśnie było w Luwrze. Pod budynek podjechał jakiś podnośnik, jacyś ludzie ubrani w stroje robocze weszli przez okno, włączył się alarm... a reakcja nastąpiła zdecydowanie zbyt późno.

Uważam, że w obiektach, w których na co dzień nie dochodzi do incydentów tego typu, tym bardziej należy regularnie ćwiczyć procedury i modele postępowania. Jeśli tego nie robimy, w chwili zagrożenia zwyczajnie nie wiemy, jak się zachować, to najlepsze nawet zabezpieczenia nie będą skuteczne.

Jakie wnioski z tego incydentu powinni wyciągnąć polscy muzealnicy, szczególnie osoby odpowiedzialne za bezpieczeństwo?

Przede wszystkim należy ćwiczyć, wykorzystując scenariusze tych zdarzeń, do których doszło w innych obiektach i mogą wydarzyć się również u nas. To podstawa. Po drugie – należy opracować, przejrzeć i zweryfikować procedury dotyczące różnych zagrożeń. Bardzo często takich procedur w ogóle nie ma, a jeśli są, to praktyka pokazuje, że w sytuacji kryzysowej i tak improwizujemy. A improwizacja to najgorszy możliwy wariant działania.

Jak pokazuje przykład Luwru, miejsca, gdzie prowadzone są prace remontowe, wymagają szczególnej uwagi. Przede wszystkim trzeba precyzyjnie uzgodnić zakres prowadzonych prac. Osoby wykonujące remont powinny mieć wyraźne identyfikatory i takie stroje, aby można je było łatwo zidentyfikować. Nie tak jak w Paryżu, gdzie ktoś bez trudu podszył się pod pracowników. Jeśli rozpoznajemy pracownika jedynie po stroju i nie mamy żadnego innego elementu identyfikacji, w takim przypadku jesteśmy bezradni.

Niezbędny jest regularny przegląd systemów zabezpieczeń. W Luwrze okazało się, że systemy działały od wielu lat, ale nikt nie zauważył, iż są przestarzałe – zarówno pod kątem oprogramowania, jak i metod weryfikacji naruszeń. Od dawna nie były przeglądane ani aktualizowane i, niestety, nie zadziałały w kluczowym momencie.

Jak ocenia Pan stopień zabezpieczenia polskich muzeów? Czy istnieje „złoty środek” chroniący tego typu obiekty?

Złoty środek nie istnieje. Każdy obiekt jest inny i dla każdego należy przeprowadzić indywidualną analizę zagrożeń, a następnie dobrać odpowiednie środki bezpieczeństwa. Trzeba pamiętać, że istnieje wiele metod i technik niwelowania ryzyka – i to od analizy zależy dobór właściwego rozwiązania.

Jeśli mamy bardzo dobre zabezpieczenia techniczne, możemy zmniejszyć liczbę pracowników ochrony fizycznej. Jeśli brakuje techniki, musimy postawić na większą obsadę. To wszystko musi się wzajemnie uzupełniać.

Po zdarzeniu w Luwrze zalecałbym wszystkim podobnym instytucjom przeprowadzenie analizy bezpieczeństwa: co działa dobrze, co wymaga uzupełnienia, a co poprawy. Taka analiza powinna być wykonywana przynajmniej raz w roku – i przepisy zresztą do tego zobowiązują. Sytuacja z Luwru pokazuje, że jest to konieczne.

Czym zabezpieczenia muzeów lub obiektów zabytkowych różnią się od zabezpieczeń innych obiektów?

Najważniejsza różnica polega na tym, że w muzeach przechowywane są bezcenne muzealia, których straty nie zrekompensuje nawet najlepsze ubezpieczenie. To dobro kulturowe narodu, które wymaga szczególnej ochrony. Dodatkowo obowiązują tu bardzo konkretne przepisy regulujące zasady zabezpieczenia.

W obiektach handlowych czy biurowych przepisy są dużo bardziej ogólne. W muzeum najłatwiej byłoby zamknąć zbiory w magazynie, a przy drzwiach postawić wartownika – ale nie o to chodzi. Muzea istnieją po to, by eksponaty pokazywać. Trzeba więc znaleźć balans: prezentować zbiory publiczności, ale jednocześnie skutecznie je chronić, bo nie każdy odwiedzający przychodzi wyłącznie po to, by podziwiać.

W wielu obiektach, takich jak centra handlowe czy zakłady należące do infrastruktury krytycznej, odchodzi się od ochrony fizycznej na rzecz zabezpieczeń technicznych. Czy w muzeach jest podobnie?

Taki trend faktycznie występuje, bo pracownik ochrony generuje stały koszt, dlatego zabezpieczenia techniczne mogą się wydawać w tym kontekście bardziej opłacalne. Jednak w muzeach nie możemy całkowicie zrezygnować z ludzi. Nawet najlepsza technologia wymaga reakcji człowieka – ktoś musi zareagować na alarm, komunikat czy sygnał systemu. W Luwrze właśnie tej reakcji zabrakło.

Można optymalizować koszty, odpowiednio dobierając proporcje między techniką a ochroną fizyczną, ale całkowite odejście od obecności człowieka byłoby błędem.

Na koniec – jaka byłaby Pana kluczowa rada dla szefów bezpieczeństwa muzeów?

Po pierwsze, należy przejrzeć i zweryfikować obowiązujące procedury. Po drugie, przeprowadzać regularne ćwiczenia, by wiedzieć, czy pracownicy znają te procedury i czy potrafią się do nich



Muzeum Historii Polski
(fragmenty wystawy i centrum monitoringu)

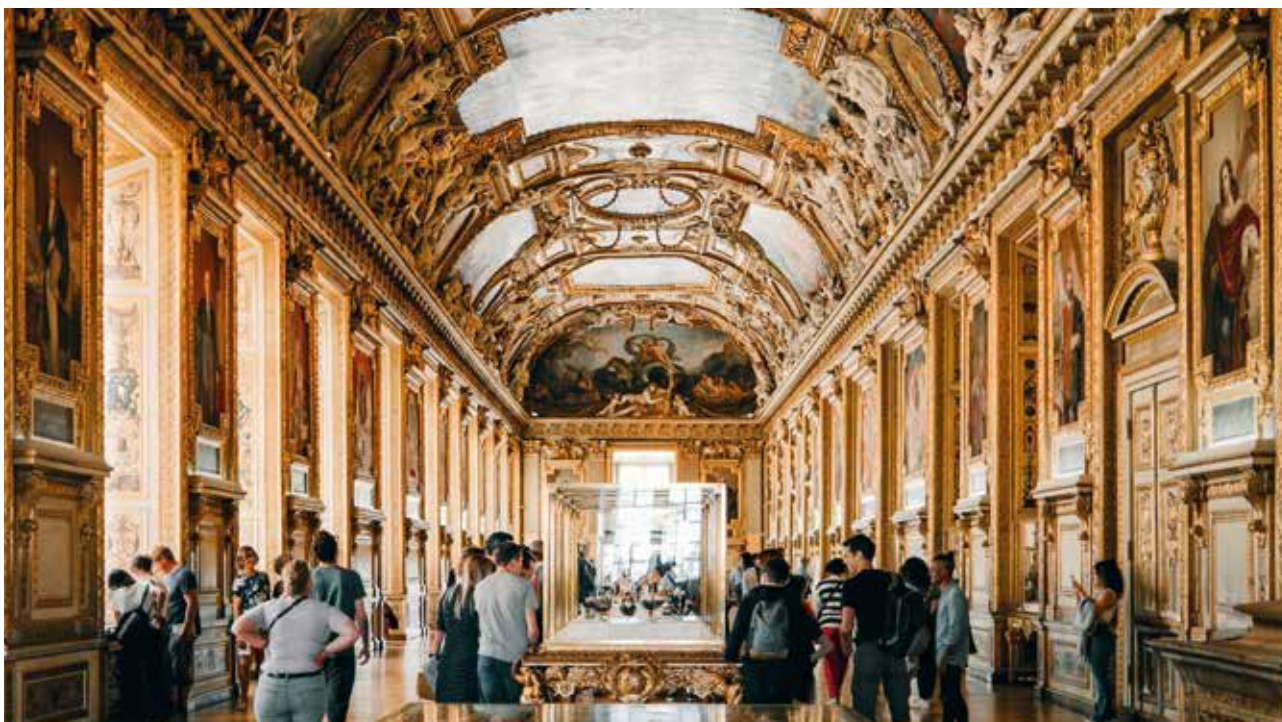
zastosować. Po trzecie, nie spoczywać na laurach. Zbudowanie systemu zabezpieczeń i podpisanie umowy z firmą ochroniarską to nie jest koniec pracy.

Systemy trzeba modernizować, aktualizować oraz – co niezwykle ważne – regularnie uruchamiać. Zdarza się, że pracownicy wyłączają zabezpieczenia, bo te „przeszkadzają”, np. z powodu fałszywych alarmów, albo są „kłopotliwe”, bo utrudniają dostęp do jakichś pomieszczeń. To absurdalne, ale częste. Tymczasem niewłączony system jest bezużyteczny, mimo że wydano na niego niejednokrotnie ogromne pieniądze.

Trzeba również kontrolować dostęp do systemów: służba ochrony powinna mieć uprawnienia użytkownika, a nie administratora. Te ostatnie powinny mieć tylko osoby upoważnione.

Niepokojące jest też to, że wiele polskich muzeów w ogóle nie ma osoby odpowiedzialnej za bezpieczeństwo. Po zdarzeniu w Luwrze należałoby postawić pytanie: jak takie obiekty są chronione, skoro nie ma nawet komu zadać podstawowych pytań o ich zabezpieczenia? To problem, którym trzeba pilnie się zająć. •

Rankiem 19 października 2025 r. muzeum Luwru, jak co dzień, przygotowywało się do przyjęcia tysięcy odwiedzających. Kustosze poprawiali białe rękawiczki, turyści polowali na najlepsze miejsce w kolejce, a kawiarnie w pobliżu tętniły życiem. Nikt nie spodziewał się, że lada moment pojawi się ekipa „renowatorów” w wersji ekstremalnej.



Bezpieczne muzea

Monika Brodawska

Zuchwali sprawcy w czteroosobowej grupie zamienili spokojny poranek w najbardziej spektakularną kradzież ostatnich lat. Dwóch mężczyzn włamało się do muzeum, używając podnośnika, podczas gdy ich dwaj współnicy czekali na zewnątrz, przygotowując ucieczkę. Złodzieje weszli przez balkonowe okno Galerii Apolla – najbardziej prestiżową część Luwru. W środku zniszczyli witryny i zabrali osiem historycznych klejnotów koronnych o wartości 102 mln dolarów, w tym skarby z czasów Napoleona i II Cesarstwa, pochodzące z XIX wieku. Cała akcja trwała zaledwie kilka minut. Agencja Reuters poinformowała, że jeden ze skradzionych klejnotów został odnaleziony tuż przy muzeum, była to korona cesarzowej Eugonii, sprawcy prawdopodobnie zgubili ją podczas ucieczki.

Bulwersujące szczegóły na temat fatalnego zabezpieczenia obiektu szybko wyszły na jaw. System kamer w kluczowych miejscach muzeum był przestarzały albo – co gorsza

– w ogóle nie istniał. Złodzieje poruszali się jak po własnym terenie, a eksperci przyznali, że część zrabowanych artefaktów może zostać bezpowrotnie utracona. A teraz wyobraźmy sobie alternatywną rzeczywistość.

Wyobraźmy sobie, że Luwr korzysta z uniwersalnego komunikatora, małej sprytniej bramy do świata monitorowania alarmów. To urządzenie błyskawicznie przekazuje sygnały z czujników i kamer do systemu monitorowania, umożliwiając natychmiastową reakcję. Kamery z funkcją analizy obrazu i wysoką rozdzielczością zauważyłyby, że renowatorzy z podnośnikiem wcale nie mają zamiaru naprawiać gzymsów. Inteligentne alerty wysłane na aplikację mobilną platformy pozwoliłyby zareagować od razu – zanim jakiegokolwiek klejnot opuściłby gablotę.

Czy tiara musiałaby przeżywać „uliczną przygodę”? Absolutnie nie. Zamiast plastikowej torby i nagłówek w gazetach byłoby jedynie rutynowe zatrzymanie intruzów,

a Galeria Apolla zostałaby majestatyczna w swojej niezakłóconej atmosferze. Dlatego muzea, galerie i instytucje kultury na całym świecie powinny traktować ochronę nie jako koszt, lecz jako inwestycję w spokój, reputację i bezpieczeństwo swoich zbiorów. Bo historia Luwru pokazuje, że złodzieje potrafią być twórczy. Pytanie brzmi: czy system ochrony jest jeszcze sprytniejszy? Bez względu na to, czy chodzi o królewskie klejnoty, bezcenne obrazy, czy unikatowe rzeźby – technologia może być tym, co sprawi, że każdy dzień w muzeum będzie spokojny. Bo w świecie sztuki liczy się aura, historia i blask. A nikt nie chce, by te wartości zniknęły – dosłownie – na podnośniku. •

Polski Związek Pracodawców Ochrona

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





Zintegrowane bezpieczeństwo w nowej fabryce Ernst & Engbring. Kompleksowa realizacja C&C Partners

Globalna Grupa TKH, do której należy również **C&C Partners**, jest organizacją zrzeszającą firmy technologiczne z całego świata, budującą przewagę rynkową dzięki współpracy, wymianie kompetencji i inwestycjom w innowacje.

Skala i doświadczenie grupy pokazują kierunek rozwoju, który w Polsce jest realizowany m.in. poprzez zaawansowane projekty, takie jak wdrożenie systemów bezpieczeństwa w nowej fabryce Ernst & Engbring GmbH (E&E).

Nowy zakład E&E – ambicja stworzenia spójnego systemu bezpieczeństwa

E&E to niemiecka firma specjalizująca się w produkcji wysokiej klasy kabli dla automatyki, instalacji przemysłowych, maszyn oraz sektora medycznego. W 2023 r. przedsiębiorstwo uruchomiło swój szósty zakład – nowoczesną fabrykę w Sierakowie koło Rawicza.

Od początku założono, że obiekt musi zostać wyposażony w spójny, skalowalny i w pełni zintegrowany system bezpieczeństwa, który obejmie zarówno ochronę fizyczną, jak i cyberbezpieczeństwo, a także zapewni bezpieczeństwo pracownikom i ciągłość procesów produkcyjnych.

Kompleksowa realizacja C&C Partners – od koncepcji po integrację

Realizacja wymagała ścisłej współpracy z generalnym wykonawcą, firmą Adamietz oraz koordynacji wielu dostawców i podwykonawców. C&C Partners była obecna od etapu

konsultacji i koncepcji, przez projekt i realizację, aż po integrację i końcowe uruchomienie systemów. Tak kompleksowe podejście pozwoliło precyzyjnie dopasować rozwiązania do potrzeb inwestora oraz stworzyć jednolitą architekturę bezpieczeństwa.



Zintegrowany system zapewniający pełną kontrolę

Zaprojektowane i wdrożone systemy objęły kontrolę dostępu iProtect, zaawansowany system monitoringu wizyjnego VDG Sense, rozwiązania interkomowe Commend, system sygnalizacji włamania i napadu UNii oraz pełną integrację przeciwpożarową z SIUP CC Winguard. Ich sercem stała się platforma PSIM+ WinGuard, która połączyła wszystkie technologie w jedno centrum zarządzania. Umożliwiło to szybką analizę zdarzeń i podejmowanie działań bez opóźnień.

Fundamentem całej infrastruktury bezpieczeństwa była również niezawodna sieć LAN i WLAN. Wydzielono odrębne środowiska dla systemów zabezpieczeń i produkcji, zastosowano nowoczesne szafy teleinformatyczne i zabezpieczono je systemem TANlock, który eliminuje nieautoryzowany dostęp do kluczowych zasobów IT.

Efekty – bezpieczeństwo, które wspiera operacyjność

Wdrożenie przyniosło fabryce nowoczesny, redundantny i skalowalny system bezpieczeństwa. Usprawniono logistykę przy bramach i punktach wejściowych, skrócono czas reakcji na zdarzenia, zintegrowano komunikację oraz zwiększono poziom ochrony pracowników, infrastruktury i procesów technologicznych. Całość została zaprojektowana w sposób skalowalny, co pozwala inwestorowi rozwijać obiekt wraz z rosnącymi potrzebami produkcyjnymi. •



C&C Partners Sp. z o.o.

ul. 17 Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl



Ogólnie acz szczegółowo – kamery MSC

Współczesne systemy dozoru wizyjnego stoją przed wyzwaniem pogodzenia dwóch sprzecznych wymagań: zapewnienia szerokiego, panoramicznego widoku sytuacyjnego oraz możliwości jednoczesnej analizy detali w wysokiej rozdzielczości. W tradycyjnym ujęciu uzyskanie szerokiego pola widzenia kosztem szczegółowości było nieuniknionym kompromisem, stąd poszukiwania rozwiązań w ekstremalnie wysokich rozdzielczościach.

Jan T. Grusznic



Dynamiczny rozwój technologii doprowadził do powstania zaawansowanej klasy urządzeń – kamer wieloprzetwornikowych (*Multi-Sensor Cameras – MSC*). Kamery MSC stanowią rozwiązanie klastrowe, łącząc od dwóch do niekiedy kilkunastu niezależnych modułów optycznych i sensorów w jednej, zintegrowanej i zwartej obudowie. Ich strategiczna rola polega na zminimalizowaniu liczby instalowanych jednostek przy jednoczesnym maksymalnym pokryciu terenu i zapewnieniu jakości obrazu niezbędnej do pracy z zaawansowaną analityką wideo. Takie podejście jest kluczowe w dozorze wielkoobszarowym: w monitoringach miejskich,

wielkopowierzchniowych obiektach handlowych, parkach logistycznych czy w infrastrukturze krytycznej.

Pierwsza generacja szerokokątnych kamer – obiektywy *fisheye* i wirtualny PTZ

Ewolucja kamer wieloprzetwornikowych szerokokątnych rozpoczęła się od kamer jednoprzetwornikowych, najczęściej wyposażonych w optykę hemisferyczną (typu *fisheye*). Kamery te, obserwujące scenę poprzez pojedynczą soczewkę, oferowały natchmiastową zaletę prawdziwego pokrycia 360 stopni bez jakichkolwiek ślepych stref. Kamery tego typu wyposażone w przetworniki wysokiej rozdzielczości wyposażono w funkcjonalność wirtualnego PTZ, który pozwala operatorowi na cyfrowe sterowanie wycinkiem w obrębie jednego, stałego, szerokiego kadru. Oprogramowanie symuluje ruch kamery obrotowej, jednocześnie zachowując ciągle nagranie całego pierwotnego pola widzenia.

Deformacje obrazu i ograniczenia pojedynczego przetwornika

Technologia ta była przełomowa, ponieważ oferowała elastyczność w manipulowaniu obrazem na materiale archiwalnym, bez utraty stałego dozoru całej sceny. To stanowi wadę tradycyjnych kamer obrotowych, które, śledząc jeden cel, tracą ciągle nadzór nad pozostałym obszarem. Jednakże, pomimo innowacji wirtualizacji, skuteczność tych systemów była nieuchronnie limitowana przez fizyczne i optyczne ograniczenia pojedynczego przetwornika. Obraz z optyki hemisferycznej jest silnie zdeformowany i wymaga cyfrowego korygowania perspektywy (*dewarping*). W wyniku tego procesu obszary na krawędzi kadru ulegają znacznemu rozciągnięciu i pikselizacji, co sprawia, że analiza odległych obiektów staje się niemożliwa.

Wpływ wielkości sensora i optyki na jakość oraz koszty

Wzrost rozdzielczości obrazu często wymaga zastosowania fizycznie większych przetworników, zwłaszcza jeśli chcemy zachować dobrą czułość przy słabym oświetleniu. Z kolei, zgodnie z prawami optyki, duże przetworniki wymuszają użycie fizycznie dużych, ciężkich i skomplikowanych zespołów soczewek. Konsekwencją tego jest nie tylko wzrost gabarytów samej kamery, ale także znaczący wzrost kosztów związanych z produkcją i instalacją. A całość ma być przystosowana do rygorów ciągłej pracy w skrajnych i dynamicznych warunkach temperaturowych, jakie panują w zewnętrznym dozorze wizyjnym.

Druga generacja szerokokątnych kamer – systemy wieloprzetwornikowe

W odpowiedzi na te potrzeby rynek przesunął się w kierunku drugiej generacji rozwiązań szerokokątnych – kamer wieloprzetwornikowych. Kamery te składają się z kilku niezależnych modułów kamerowych w jednej obudowie. Każdy moduł ma własny przetwornik obrazu i niezależny układ optyczny, które są ze sobą połączone w celu stworzenia jednolitej, panoramicznej sceny. Centralny układ przetwarzający w takich urządzeniach jest odpowiedzialny za zarządzanie tymi niezależnymi strumieniami danych oraz za zaawansowane łączenie obrazów (*stitching*), eliminując widoczne przejścia między modułami.



Jest to podejście, w którym moc obliczeniowa i zaawansowane algorytmy przetwarzania są wykorzystywane do stworzenia obrazu lepszego niż suma jego części. Jedną z największych przewag operacyjnych kamer MSC jest znaczne uproszczenie infrastruktury. Mimo iż fizycznie urządzenie składa się z wielu kamer, dla sieci i systemu rejestracji (VMS) jest ono traktowane jako jedna jednostka, zarządzana pod jednym adresem IP i mająca jeden interfejs graficzny (GUI). To drastycznie redukuje złożoność wdrożenia, zmniejsza potrzebę okablowania oraz minimalizuje liczbę licencji VMS wymaganych do obsłużenia szerokiego obszaru. W przypadku dużych instalacji, takich jak parki logistyczne czy miejskie sieci dozoru, te oszczędności infrastrukturalne i na robociznie stają się kluczowym czynnikiem przy podejmowaniu decyzji.

Głębia ostrości jako centralny problem optyki w dozorze

Kamery MSC doskonale radzą sobie z wyzwaniem optycznym związanym z jednoczesną obserwacją bliskiego i dalekiego planu. W architekturze wieloprzetwornikowej bowiem inżynierowie świadomie zdecydowali się rozłożyć wyzwanie optyczne na kilka mniejszych modułów, eliminując problem spłylenia głębi ostrości (*Depth of Field – DOF*). Głębia ostrości definiuje odległość między najbliższym a najdalszym obiektem, które są akceptowalnie ostre na zarejestrowanym obrazie.

Głębia ostrości jest determinowana przez trzy główne czynniki optyczne:

- 1. Długość ogniskowej obiektywu:** Im dłuższa ogniskowa (większe zbliżenie), tym mniejsza głębia ostrości.
- 2. Wartość przysłony:** Mniejsza przysłona (większa wartość F) zwiększa głębię ostrości (do pewnego momentu, gdy zbyt mała szczelina zwiększa efekt dyfrakcji – po więcej zapraszam do artykułu *Magia wysokich rozdzielczości* z nr 5/2017 „a&s Polska”).
- 3. Rozmiar matrycy (sensora):** Mniejsze matryce automatycznie zapewniają większą głębię ostrości, choć kosztem jakości przy słabym świetle.

Ograniczenia kamer jednoprzetwornikowych w kontroli bliskiego i dalekiego planu

W przypadku monitorowania granicy terenu, np. linii ogrodzenia, kamera musi obserwować elementy zarówno bliskie punktu kamerowego (gdzie może dojść do sabotażu), jak i dalekie (horyzont i strefa podejścia). Jeśli zastosujemy kamerę jednoprzetwornikową o szerokim kącie (krótka ogniskowa), uzyskamy dużą głębię ostrości, co oznacza, że i bliskie okolice punktu kamerowego, i horyzont mogą wydawać się „ostre”. Jednakże duża DoF w tym przypadku jest osiągnięta kosztem jakości detali na dalekim planie. Krótka ogniskowa powoduje, że odległe obiekty (np. intruz w odległości 100 m) będą reprezentowane przez zbyt małą liczbę pikseli, aby móc przeprowadzić skuteczną analizę rozpoznawania.

Z kolei próba uzyskania szczegółu na dalekim planie za pomocą dużej ogniskowej (teleobiektywu) dramatycznie redukuje głębię ostrości. W efekcie ostrość ustawiona na horyzoncie sprawi, że bliski plan całkowicie zniknie w tzw. martwej strefie, uniemożliwiając detekcję np. prób sabotażu. Kamera jednoprzetwornikowa jest zatem zmuszona do wyboru: albo szeroki ogląd sytuacyjny (kosztem detali), albo szczegółowy widok (kosztem pokrycia i DoF).



MSC – jedyne rozwiązanie pozwalające na równoczesne strefy ostrości

Kamera wieloprzetwornikowa stanowi jedyną technologiczną odpowiedź na to fizyczne ograniczenie optyki. Wykorzystując swoją kluczową przewagę – niezależne układy optyczne, mogące tworzyć równoczesne, niezależne strefy ostrości. Dzięki niezależnym układom optycznym, możliwe jest jednoczesne utrzymanie pełnej ostrości na obiektach znajdujących się na różnych planach. Jeden moduł może być zoptymalizowany pod kątem bliższej obserwacji, wykorzystując mniejszy przetwornik i krótszą ogniskową, co naturalnie zwiększa głębię ostrości w tym sektorze. Inny moduł może być ustawiony na horyzont. W efekcie kamera wieloprzetwornikowa może obserwować bliskie otoczenie punktu montażowego, a także daleki obszar, bez ponoszenia konsekwencji wynikających z ograniczonej głębi ostrości dla kamer jednoprzetwornikowych.

Zastosowania MSC: miasta, handel, logistyka, infrastruktura

Kamery MSC są idealne w projektach miejskich i lotniskowych, gdzie konieczny jest stały monitoring dynamicznych, rozległych scen. Instalowane na skrzyżowaniach, dużych placach publicznych lub dworcach, kamery te działają jak „oczy dookoła głowy”, zapewniając pełne pokrycie ciągów komunikacyjnych. Zdolność



do jednoczesnego rejestrowania ogólnego ruchu i dostarczania szczegółów z każdego kierunku w wysokiej rozdzielczości (np. do analizy ruchu czy identyfikacji pojazdów) czyni je efektywniejszymi niż instalacja wielu kamer stałopozycyjnych lub pojedynczej kamery PTZ.

W sektorze logistycznym, MSC znajdują zastosowanie w obserwacji rozległych terenów, takich jak parkingi, obszernych magazynów, placów składowania i parków maszynowych. Możliwość objęcia całego parkingu lub hali produkcyjnej jedną kamerą znacząco upraszcza instalację.

Wbudowane funkcje AI pozwalają na precyzyjne ustawienie granic monitorowanego obszaru. W przypadku obiektów handlowych MSC gwarantują monitorowanie dużego obszaru sklepu, jednocześnie zapewniając wysoką niezawodność i możliwość podglądu na żywo.

TCO jako kluczowy parametr inwestycyjny

Dla decydentów i menedżerów bezpieczeństwa ocena inwestycji w system dozoru nie może ograniczać się wyłącznie do analizy początkowego kosztu zakupu (*CapEx*). Kluczowym wskaźnikiem jest Całkowity Koszt Posiadania (*Total Cost of Ownership – TCO*), który uwzględnia koszty operacyjne (*OpEx*), utrzymania i potencjalnych awarii w całym cyklu życia rozwiązania. Choć kamery

MSC mają wyższą cenę jednostkową niż jednoprzetwornikowe kamery IP, ich architektura prowadzi do znaczących oszczędności w TCO. Konsolidacja czterech lub więcej kamer w jednej obudowie przekłada się na wymierne oszczędności finansowe i operacyjne:

- **Redukcja CapEx na Infrastrukturę:** Zamiast czterech oddzielnych instalacji wystarczy jedna. Oszczędności obejmują okablowanie, redukcję wymaganej liczby portów PoE w switchach sieciowych oraz eliminację konieczności zakupu indywidualnych zasilaczy.

- **Redukcja OpEx na Licencjonowanie:** Wiele systemów VMS (*Video Management System*) lub NVR (*Network Video Recorder*) licencjonuje każde fizyczne urządzenie osobno. Ponieważ MSC są traktowane jako jedno urządzenie sieciowe (jeden adres IP), koszty licencji VMS mogą zostać zredukowane wielokrotnie. W dużych wdrożeniach na 10, 50 lub więcej punktów kamerowych, ta oszczędność na licencjach jest znacząca i przewyższa początkowy wydatek na sprzęt.

Horyzont rozwoju – integracja wielosensorowa i technologie obronne

Oprócz standardowego dozoru wizyjnego koncepcja macierzy sensorów jest rozwijana w kierunku integracji z innymi technologiami. W sektorze obronnym i ochrony granic systemy łączą podejście MSC z technologią termowizyjną, osiągając operacyjny zasięg detekcji liczący dziesiątki kilometrów. W takich systemach są często częścią większego, zintegrowanego rozwiązania, współpracując z radarami i zaawansowanymi platformami zarządzania bezpieczeństwem.

Podsumowanie – MSC jako nowy standard profesjonalnego dozoru

Rozwój technologiczny zmierza w kierunku dalszej integracji sensorów i pogłębienia możliwości analitycznych. Optyka z macierzą soczewek i rozwój zaawansowanych technik cyfrowego łączenia obrazów przyczyniają się do poprawy precyzji, zmniejszenia zniekształceń i zwiększenia efektywności kamer w środowiskach, w których szczególnie i szerokie pole widzenia muszą być dostarczane jednocześnie.

Kamery wieloprzetwornikowe stanowią kamień milowy w ewolucji profesjonalnego dozoru wizyjnego, wychodząc na przeciw potrzebie uzyskania panoramicznego oglądu sytuacyjnego bez kompromisów w zakresie szczegółowości i analityki. To przejście od kamer jednoprzetwornikowych typu *fisheye* (gdzie utrata rozdzielczości była nieunikniona) do modularnych macierzy sensorów z niezależną optyką radykalnie zmieniło możliwości nadzoru na dużych obszarach. Producenci uchylają rąbka tajemnicy i wskazują dalsze perspektywy rozwoju kamer wieloprzetwornikowych, które obejmują dalszą konwergencję technologiczną: integrację z sensorami termowizyjnymi i radarowymi, rozwój algorytmów głębokiego uczenia maszynowego dla jeszcze większej precyzji w rozpoznawaniu i śledzeniu obiektów, a także automatyzację procesów zarządzania bezpieczeństwem. MSC ugruntowują swoją pozycję jako nowy standard, umożliwiający skuteczniejszą i bardziej proaktywną ochronę mienia i osób. •

Jan T. Grusznicki
redaktor „a&s Polska”



Kamery panoramiczne BCS Line i BCS Point

Kamery panoramiczne stają się coraz popularniejszym wyborem w nowoczesnych systemach monitoringu przede wszystkim dzięki możliwości zastąpienia kilku tradycyjnych kamer jednym urządzeniem. Rozwiązanie to znacząco redukuje koszty instalacji oraz upraszcza jej wykonanie. Co istotne, kamery panoramiczne BCS zajmują tylko jeden kanał w rejestratorze, co pozwala jednocześnie oszczędzać dostępne kanały oraz przestrzeń dyskową.

W praktyce zastosowanie kamer panoramicznych zwiększa poziom bezpieczeństwa systemu. Osoba próbująca uniknąć obserwacji ma znacznie mniejszą szansę na opuszczenie pola widzenia, a operator otrzymuje pełny obraz sytuacji bez konieczności przełączania się między wieloma kamerami. Dodatkowo panoramiczny obraz rozszerza

możliwości działania funkcji inteligentnej analizy – pozwala wykrywać osoby i pojazdy na większym obszarze bez potrzeby instalowania dodatkowych urządzeń.

Kamery panoramiczne BCS Line oraz BCS Point wyposażone są także w technologię aktywnego odstraszania (sygnalizację świetlną i dźwiękową), innowacyjną technologię NightColor 2.0 oraz oświetlacze podczerwieni lub światła LED, co zapewnia wysoką jakość nagrań niezależnie od warunków oświetleniowych.

BCS oferuje kamery panoramiczne dwóch rodzajów.

1. Kamery wieloprzetwornikowe – tworzą pojedynczy, szerokokątny obraz na podstawie strumieni z kilku obiektywów. Mogą oferować różne zakresy obserwacji, np.:

- BCS-P-PTIP2X2FCL3-Ai1 – obserwacja 180° w poziomie i 47° w pionie,



- BCS-L-PTIP4X8FSR3-Ai2 – obserwacja 180° w poziomie i 100° w pionie.

2. Kamery z jednym obiektywem – wykorzystujące wypukłą soczewkę typu *fisheye*, która umożliwia bardzo szeroką obserwację przy użyciu jednego przetwornika.

Modele BCS-P-PTIP1x5FWR2-Ai1 oraz BCS-P-PEIP1x8FWR2-Ai1 zapewniają obserwację 180° w poziomie oraz 100° w pionie.

Podsumowując, kamery panoramiczne znacząco podnoszą skuteczność monitoringu, jednocześnie obniżając koszty całego systemu. Dzięki szerokiemu polu widzenia, zaawansowanym funkcjom inteligentnej analizy oraz technologiom poprawiającym jakość obrazu oferują wysoki poziom bezpieczeństwa przy minimalnej liczbie urządzeń. •

Więcej na: www.bcs.pl

Panoramiczne spojrzenie na bezpieczeństwo – kamera GANZ GENSTAR w praktyce

W segmencie kamer panoramicznych 180° coraz większe znaczenie mają modele, które łączą szerokie pole widzenia z realną wartością dodaną w postaci analityki i wysokiej jakości obrazu. Do tej grupy należy kamera GANZ GENSTAR ZN8-80X2B8F28DT-J4, zaprojektowana jako rozwiązanie „jedno urządzenie – pełne pokrycie przestrzeni”. Dzięki temu może zastępować kilka tradycyjnych kamer, redukując koszty instalacji i upraszczając zarządzanie systemem monitoringu.

Model oferuje 8 Mpix panoramicznego obrazu (4608x1728 przy 30 kl/s), co przekłada się na wysoki poziom detali kluczowych w nadzorze stref wejścia, kas czy ciągów komunikacyjnych. W porównaniach rynkowych GENSTAR wyróżnia się wyższą efektywną rozdzielczością głównego strumienia oraz dłuższym zasięgiem IR – do 30 m przy dodatkowym świetle białym do 20 m, co zapewnia czytelność materiału również nocą.

Co warto podkreślić, panoramiczne ujęcie 180° eliminuje martwe strefy bezpośrednio pod kamerą – typowe dla klasycznych obiektywów szerokokątnych. W połączeniu z precyzyjną analityką IVS GenSTAR, obejmującą m.in. przecięcie linii, wtargnięcie czy śledzenie kierunku ruchu, stanowi to wyjątkowo skuteczny sposób monitorowania sklepów, przejść i magazynów, zwłaszcza w kontekście minimalizowania strat i zapobiegania kradzieżom.

Jednym z najmocniejszych atutów kamery jest rozbudowana analityka IVS 2.0: rozpoznawanie osób i pojazdów, analiza zachowań, liczenie osób oraz mapy ciepła. To funkcje, które w realnych wdrożeniach pozwalają nie tylko zwiększyć bezpieczeństwo, ale również analizować przepływ użytkowników czy efektywność przestrzeni – szczególnie w retailu i obiektach usługowych.

Warto zwrócić uwagę na obsługę dwóch osobnych obrazów – każdy w 5 Mpix – co daje elastyczność konfiguracji, niedostępną w wielu konkurencyjnych modelach.



Dodatkowo kamera oferuje lokalny zapis na microSD do 1 TB, co umożliwia tworzenie kopii bezpieczeństwa na miejscu instalacji.

Istotnym elementem jest również zgodność z normą NDAA, ważna w projektach instytucjonalnych i przetargach wymagających określonych standardów cyberbezpieczeństwa.

GANZ GENSTAR ZN8-80X2B8F28DT-J4 to kamera, która w przeglądarce rozwiązań panoramicznych wyróżnia się połączeniem szerokiego pola widzenia, wysokiej jakości obrazu i praktycznej analityki AI. Sprawdza się zarówno jako narzędzie ochrony, jak i platforma do zaawansowanej analizy ruchu użytkowników – szczególnie tam, gdzie liczy się jednocześnie kontrola przestrzeni i optymalizacja kosztów. •

Więcej na: www.cbcpoland.pl



i-PRO WV-S85 i WV-X86: nowy standard monitoringu

Kamery wieloprzetwornikowe i-PRO serii WV-S85 oraz hybrydowe modele serii WV-X86 (multi-sensor + PTZ) tworzą kompletne rozwiązanie dla najbardziej wymagających systemów. Łączą najwyższą jakość, szeroki zasięg obserwacji, zaawansowaną analitykę Edge AI, otwartą architekturę oraz najwyższy poziom cyberbezpieczeństwa – wszystko z myślą o bezpiecznej, wieloletniej i bezproblemowej eksploatacji systemów.

Edge AI od i-PRO analizuje obraz bezpośrednio w kamerze, odciążając serwery i skracając czas reakcji. Seria WV-X86 wprowadza środowisko Docker na poziom urządzenia, dzięki czemu można instalować dedykowane aplikacje AI od i-PRO i partnerów – dziś i w przyszłości, bez

wymiany sprzętu. Co więcej, za pomocą kamer serii X można dodać inteligentną analitykę (np. liczenie osób, rozpoznawanie atrybutów) do strumieni z kamer pozbawionych funkcji AI, pozwalając ekonomicznie unowocześnić istniejący system. Otwarta platforma ułatwia integrację z rozwiązaniami firm trzecich i dopasowanie do indywidualnych scenariuszy.

Bezpieczeństwo danych i systemu jest kluczowe. Kamery wyposażono we wbudowany, certyfikowany FIPS 140-2 Level 3 SecureElement do ochrony kluczy szyfrujących oraz podpisane oprogramowanie układowe, które zapobiega nieautoryzowanym modyfikacjom. Zgodność z Sekcją 889 ustawy NDAA i TAA potwierdza zweryfikowane pochodzenie urządzeń. Dodatkowo i-PRO oferuje aż 7-letnią gwarancję na wybrane modele, znacząco ograniczając koszty utrzymania.



i-PRO Co., Ltd., powstała w 2019 roku jako niezależna firma wywodząca się z ponad 60 lat doświadczeń Panasonic, jest dziś globalnym liderem w technologiach bezpieczeństwa, ochrony i obrazowania medycznego.

Wybierając kamery i-PRO serii WV-S85 i WV-X86, inwestujesz w inteligentne, przyszłościowe i bezpieczne rozwiązania. Aby poznać pełną ofertę i dobrać właściwą konfigurację, skontaktuj się z oficjalnym premium dystrybutorem w Polsce – firmą CCTV Baltic. •

Więcej na: www.cctvbaltic.com

Przeгляд kamer panoramicznych Panomera®

Nowość – kamera Panomera® V8 to zaawansowany system wizyjny AI łączący multifokalną technologię z ośmioma zintegrowanymi przetwornikami. Kamera oferuje płynny, pozbawiony martwych pól widok 180°, dzięki czemu jedno urządzenie może nadzorować bardzo duże obszary. Ośmiem obiektywów i przetworników tworzy jeden spójny obraz, co znacząco zwiększa precyzję analiz oraz niezawodność systemów bezpieczeństwa.

Największą przewagą Panomera® V8 jest monitoring pełnej sceny, co eliminuje typowe ograniczenia analityki wideo, takie jak brak ciągłości danych czy nakładanie się obrazu. System zapewnia idealne warunki do pracy zaawansowanych algorytmów, od analizy incydentów, przez śledzenie przepływu ludzi i pojazdów, po monitorowanie procesów operacyjnych. Umożliwia szybkie wyszukiwanie osób i przedmiotów, dokładną analizę ruchu oraz znacząco redukuje liczbę fałszywych alarmów. Dzięki



temu kamera wspiera zarówno bezpieczeństwo, jak i optymalizację działań na dużych terenach.

Kolejną panoramiczną kamerą od Dallmeier jest Panomera® S4 Perimeter. To wieloprzetwornikowe urządzenie zaprojektowano do rejestrowania wąskiego pasa wzdłuż ogrodzenia (strefy sterylnej). Zapewnia rozdzielczość 200 Mpix na potrzeby zintegrowanej analizy wideo z wykorzystaniem sztucznej inteligencji.

Zastosowanie tego typu kamer znacznie zmniejsza wymagania infrastrukturalne. Tam, gdzie wcześniej konieczne było zastosowanie kilku kamer megapikselowych, teraz wystarczy jeden system wieloprzetwornikowy Panomera®.

Wszystkie kamery Panomera® są produkowane w Niemczech, z wykorzystaniem własnych modeli AI i pełną kontrolą nad danymi, co gwarantuje wysokie standardy zarówno jakości, cyberbezpieczeństwa, jak i niezawodności. Dzięki możliwości zastąpienia wielu tradycyjnych kamer jednym urządzeniem system znacząco obniża koszty infrastruktury i całkowity koszt posiadania.

Kamery Panomera® V8, S8 i S4 Perimeter znakomicie sprawdzają się w inteligentnych miastach, na lotniskach, stadionach, w logistyce, portach oraz w przemyśle i infrastrukturze krytycznej. •

Więcej na: www.urkom.pl



Oferta kamer panoramicznych VIVOTEK

VIVOTEK oferuje szeroką gamę kamer panoramicznych, które można klasyfikować nie tylko według typu obudowy, lecz także ze względu na charakter i jakość generowanego obrazu.

Pierwszą grupę stanowią kamery panoramiczne 180°, tworzące szerokokątny obraz z jednego przetwornika o rozdzielczości 2, 5 lub 8 Mpix (seria CC), z dwóch przetworników zapewniających obraz 8 Mpix, a także z czterech przetworników pozwalających uzyskać obraz o wysokiej szczegółowości w rozdzielczości 18 Mpix (seria MS).

Drugą grupę tworzą dobrze znane kamery typu „rybie oko” (*Fisheye*), wyposażone w przetworniki o rozdzielczości od 5 do 12 Mpix. Dostępne są w wersjach zarówno wewnętrznych, jak i zewnętrznych – z promiennikiem IR lub bez – a także w wariantach natynkowych i podtynkowych (seria FE).

Trzecią grupę stanowią panoramiczne kamery wielokierunkowe, oferowane w konfiguracjach 2x5 Mpix, 2x8 Mpix oraz 4x5 Mpix (seria MA).

Zakres zastosowań kamer panoramicznych jest szeroki. Kamery serii CC idealnie sprawdzają się w miejscach, gdzie zależy nam na uzyskaniu szerokiego kadru z jednego urządzenia przy zachowaniu ogólnego poziomu obserwacji, np. na stacjach benzynowych, w hotelowych lobby czy w pomieszczeniach biurowych. Kamery serii MS doskonale nadają się do monitoringu rozległych, otwartych przestrzeni, takich jak parkingi czy stadiony. Urządzenia z serii FE znajdują zastosowanie zarówno wewnątrz budynków, jak i na skrzyżowaniach, umożliwiając objęcie dużego obszaru dzięki centralnemu montażowi jednej kamery. Z kolei kamery serii MA są świetnym rozwiązaniem w systemach, w których chcemy ograniczyć liczbę urządzeń, a jednocześnie uzyskać niezależne, wysokiej jakości obrazy z każdego przetwornika.

Czym zatem kamery panoramiczne przewyższają klasyczne rozwiązania? Przede wszystkim pozwalają znacząco

zmniejszyć liczbę koniecznych urządzeń. Jedna kamera panoramiczna może skutecznie zastąpić od dwóch do czterech standardowych kamer, co przekłada się na krótszy czas instalacji, mniejszą ilość okablowania oraz redukcję liczby niezbędnych licencji. Wszystkie opisane modele wyposażone są ponadto w zaawansowane funkcje analityczne, podnoszące efektywność systemu monitoringu. •

Więcej na www.vivotek.com





Bezpieczeństwo jutra: przyszłość ochrony fizycznej

Rynek ochrony fizycznej w Polsce wchodzi w etap głębokiej transformacji. Rosnąca presja kosztowa, wymagania dotyczące jakości oraz konieczność integracji nowoczesnych technologii sprawiają, że branża musi redefiniować swoje standardy. O kierunku, w jakim rozwija się profesjonalna ochrona - dziś i w najbliższych latach - rozmawiamy z **Markiem Skowronkiem**, członkiem Zarządu w Securitas Polska, Chief Commercial & Solutions Officer.



Czy na polskim rynku ochrony fizycznej obserwujemy realną zmianę – od presji cenowej do realnego wartościowania jakości?

Trudne pytanie. Myślę, że wciąż na rynku ochrony funkcjonuje przekonanie, że cena jest jednym z głównych wyznaczników, ponieważ firmy bardzo mocno patrzą na koszty i nieustannie szukają oszczędności. Dlatego jednym z głównych kryteriów pozostaje cena. Widzimy dwie grupy klientów. Dla jednych cena nie jest najważniejsza – mam na myśli klientów korporacyjnych, dla których których kluczowa jest jakość, kwalifikacje pracowników ochrony oraz stała inwestycja w ich rozwój.

Drugą grupą są przedsiębiorstwa w segmencie SME (*Small and Medium Enterprise*), dla których głównym wyznacznikiem jest cena. To na jej podstawie podejmowane są decyzje zakupowe, nawet jeśli w zapytaniach pojawiają się dodatkowe elementy. Tyle tylko, że ich procentowy udział jest naprawdę niewielki – rzędu 10%-20%, a około 80% stanowi cena.

A jak to się ma w kontekście ostatnich i kolejnych zapowiadanych podwyżek płacy minimalnej? Czy w tej rzeczywistości możliwe jest utrzymanie jakości świadczonych usług?

Myślę, że tak, firmy będą dążyć do utrzymania jakości. Wzrost minimalnego wynagrodzenia w najbliższym roku jest stosunkowo niewielki w porównaniu z latami poprzednimi. Według mnie nie spowoduje to tak drastycznych cięć, np. w zakresie optymalizacji roboczogodzin. Coraz trudniej jednak będzie utrzymać wysoką jakość za minimalne wynagrodzenie. Tym

bardziej, że problem dotyczy nie tylko branży ochrony, ale w ogóle całego kraju.

Jednym z większych wyzwań jest demografia – mamy coraz mniej osób aktywnych zawodowo. Trudno jest dziś pozyskać pracownika, który chce związać się z branżą na dłużej i w którego można inwestować.

Porozmawiamy jeszcze o technologii, a konkretnie o sztucznej inteligencji. Trend wykorzystania AI jest coraz silniejszy w zabezpieczeniach technicznych. A jak to wygląda w przypadku firm ochrony fizycznej? Czy także wykorzystujecie sztuczną inteligencję?

To dziś jest nieodzowny element. Szansą dla wszystkich firm, nie tylko z sektora ochrony, jest cyfryzacja i inwestycje w technologię, w tym w sztuczną inteligencję. Będziemy z niej coraz częściej korzystać. Jednym z przykładów, gdzie AI jest w zasadzie nieodzowne, są algorytmy AI w kamerach – stosujemy zaawansowaną analizę obrazu, która znacznie podnosi skuteczność systemu monitoringu.

Na przykładzie danych zebranych przez Securitas można powiedzieć, że dzisiaj ponad 96% wszystkich alarmów z kamer, korzystających z zaawansowanej analizy, jest weryfikowanych przez AI. To pozwala optymalizować czynnik ludzki. Nie musimy wprowadzać dodatkowych posterunków, by obsługiwać większą liczbę kamer, bo analizę wykonuje sztuczna inteligencja. To jest kierunek, w którym idziemy i tego oczekują również przedsiębiorcy.

W Securitas AI zagościła na dobre w wielu obszarach, np. proces rekrutacji jest

wspierany przez sztuczną inteligencję. AI potrafi zweryfikować profil kandydata i ocenić, czy pasuje do danej roli i stanowiska, na które aplikuje. Możemy też analizować cały proces rekrutacyjny, podejmować trafniejsze decyzje i lepiej planować zasoby kadrowe, uwzględniając potrzeby klientów.

Czy możemy polegać na AI?

Musimy potrafić odróżniać poprawne odpowiedzi od ewentualnych halucynacji modeli. Z czasem będziemy także zadawać lepsze pytania, bo to właśnie w tym tkwi sedno skutecznej pracy z AI.

Wiele zmieni się w najbliższych latach. W Securitas korzystamy z wydzielonej wersji ChatGPT, dzięki czemu dane naszych klientów pozostają w pełni chronione. Nie używamy otwartych narzędzi – pracujemy na własnym, zamkniętym środowisku.

Już teraz, gdy otrzymujemy kontrakt, AI potrafi przeanalizować go w bardzo krótkim czasie. To samo narzędzie wskazuje potencjalne ryzyka oraz sugeruje rekomendacje zmian dla klienta. Dzięki temu czas reakcji znacząco się skraca, co samo w sobie stanowi dużą wartość. •

O tym, jakich zmian można spodziewać w najbliższych latach, czy będziemy obserwować konsolidację na tym rozdrobnionym polskim rynku, przeczytasz w dalszej części wywiadu dostępnej na portalu aspolska.pl.



Securitas Polska

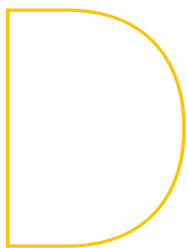
Postępu 6
02-676 Warszawa
securitas@securitas.pl



Strategiczne podejście do projektów bezpieczeństwa

Bezpieczeństwo w firmach coraz częściej przestaje być kosztem, a staje się inwestycją. Duże organizacje już dawno zauważyły, że pojedyncze działania, takie jak instalacja systemu monitoringu wizyjnego czy wdrożenie polityki cyberbezpieczeństwa, nie wystarczą. Potrzebne jest strategiczne podejście do projektów bezpieczeństwa, które łączy technologię, procesy i ludzi.

Daniel Kamiński



Dlaczego warto strategicznie podchodzić do bezpieczeństwa? Takie podejście oznacza planowanie na lata, a nie na kwartał. Firmy, które traktują bezpieczeństwo doraźnie, często ponoszą wyższe koszty, ponieważ awarie, incydenty czy błędy wdrożeniowe wymagają kosztownych poprawek. Z kolei organizacje planujące działania w perspektywie długoterminowej zyskują między innymi:

- większą przewidywalność wydatków,
- lepszą ochronę kluczowych procesów,
- spójność pomiędzy bezpieczeństwem fizycznym a cyberbezpieczeństwem.

To właśnie strategiczne podejście do bezpieczeństwa sprawia, że systemy nie tylko chronią, ale także wspierają rozwój biznesu.

Projekty bezpieczeństwa w dużych firmach: doświadczenia i wyzwania

Podczas współpracy z dużymi firmami zauważyłem, że każdy projekt bezpieczeństwa jest inny, ale wyzwania często się powtarzają. Do najczęstszych należą:

- **brak spójnej wizji** – różne działy wdrażają swoje rozwiązania bez koordynacji,
- **skupienie na sprzęcie zamiast na procesach** – firma kupuje technologię, ale nie tworzy procedur,
- **niedoszacowanie kosztów utrzymania** – budżet zakłada instalację, ale nie uwzględnia serwisu czy aktualizacji.

Jednocześnie dobrze prowadzone projekty pokazują, że przy odpowiednim zarządzaniu można uzyskać realne efekty: lepszą ochronę danych, krótszy czas reakcji w kryzysie czy większą świadomość pracowników.

Rola doradcy i wsparcie inwestora

Jednym z kluczowych elementów skutecznych wdrożeń jest rola doradcy w projektach bezpieczeństwa. Duży inwestor rzadko ma czas i wiedzę, aby samodzielnie nadzorować wszystkie etapy. Zewnętrzny ekspert może:

- wspierać inwestora w trakcie realizacji wdrożenia,
- reprezentować interesy firmy wobec dostawców,
- wskazywać obszary ryzyka pomijane w standardowym podejściu.

Ważnym etapem jest też transfer wiedzy po wdrożeniu i okresowe kontrole. Bez tego system szybko „starzeje się” i przestaje działać zgodnie z założeniami. Firmy, które włączają szkolenia, cykliczne audyty i przeglądy, budują trwałą wartość zamiast kupować „jednorazowe” rozwiązanie.

Konwergencja bezpieczeństwa: łączenie IT i OT

W dużych organizacjach bezpieczeństwo nie kończy się na kamerach czy firewallach. Coraz większą rolę odgrywa konwergencja

bezpieczeństwa: integracja systemów fizycznych (ochrona, monitoring, kontrola dostępu) z obszarem IT i OT.

- W fabrykach oznacza to połączenie ochrony fizycznej z cyberbezpieczeństwem systemów produkcyjnych.
- W biurach, integrację kontroli dostępu, zarządzania incydentami i monitoringu wizyjnego z siecią IT.

Z mojego doświadczenia wynika, że firmy, które wprowadzają konwergencję bezpieczeństwa, nie tylko ograniczają ryzyko, ale też lepiej wykorzystują dane. Raporty z systemów mogą wspierać zarządzanie procesami, a nie służyć wyłącznie reagowaniu na zagrożenia.

Czego uczy współpraca z dużymi firmami?

Najważniejsze wnioski z moich projektów z dużymi organizacjami to:

- bezpieczeństwo musi być elementem strategii, nie dodatkiem,
- inwestor potrzebuje doradcy, który rozumie zarówno technologię, jak i biznes,
- efekty strategicznego podejścia do bezpieczeństwa są widoczne nie od razu, ale procentują w długim okresie,
- wartość dodaną daje partnerstwo – od analizy ryzyka, przez wdrożenie, aż po utrzymanie i rozwój systemu.

Efekty strategicznego podejścia do bezpieczeństwa

Współpraca strategiczna oznacza więcej niż „projekt zakończony sukcesem”. To stały proces, w którym:

- firma unika powtarzania kosztownych błędów,
- zyskuje elastyczność w dostosowywaniu systemów do zmian w otoczeniu,
- buduje przewagę konkurencyjną poprzez stabilność i odporność.

Dlatego właśnie **efekty współpracy strategicznej w bezpieczeństwie** można podsumować jednym zdaniem: bezpieczeństwo przestaje być kosztem, a staje się wartością biznesową.

Podsumowanie

Strategiczne podejście do projektów bezpieczeństwa to inwestycja w długofalowe partnerstwo, transfer wiedzy i ciągłe doskonalenie. To podejście, które sprawdza się szczególnie w dużych firmach, ale coraz częściej jest potrzebne także w średnich i mniejszych organizacjach. Wdrożenie systemu to dopiero początek – prawdziwa wartość powstaje wtedy, gdy bezpieczeństwo wpisane jest w DNA całej firmy.



Daniel Kamiński

Absolwent kierunku Telekomunikacji WAT oraz Kierowania Systemami Teleinformatycznymi AON. Specjalizuje się w rozwiązaniach ICT, systemach zabezpieczeń i cyberbezpieczeństwie, łącząc wiedzę technologiczną z doświadczeniem w zarządzaniu oraz wdrażaniu innowacyjnych rozwiązań. Od ponad 20 lat dzieli się swoją wiedzą na łamach czasopism branżowych. Wykładowca PISA, członek sekcji zabezpieczeń technicznych PIO.



Milestone Technology Day Poland 2025: technologia, która rozumie świat

Przyszłość technologii wizyjnej zależy nie tylko od tempa rozwoju innowacji, lecz także od siły partnerstw, które potrafią je wdrażać i rozwijać. Z takim przesłaniem 30 października w Warszawie odbył się **Milestone Technology Day Poland 2025** – wydarzenie, które połączyło ekspertów, partnerów i użytkowników rozwiązań wizyjnych, skupionych na wspólnym budowaniu efektywnych, skalowalnych i inteligentnych ekosystemów.

– *Polski rynek jest jednym z najbardziej dynamicznych i najszybciej rozwijających się w naszym regionie, a Milestone Technology Day to kluczowa okazja do nawiązania kontaktu z naszą społecznością i poszerzenia sieci współpracy. Chodzi przede wszystkim o zgromadzenie naszych partnerów, klientów i kanału sprzedaży, aby dzielić się wiedzą, inspirować współpracę oraz budować relacje napędzające innowacje i długoterminowy rozwój* – powiedziała Borislava Kenarova, Regionalna Dyrektorka Sprzedaży na Europę Wschodnią, CIS i Izrael w Milestone Systems.

Podczas wydarzenia eksperci pokazali, jak technologia obrazu wychodzi daleko poza tradycyjny monitoring wizyjny. Pod hasłem **„Get ready to change the perceptions of video technology”** uczestnicy mogli przekonać się, że systemy wizyjne stają się dziś źródłem wartościowych danych wspierających decyzje strategiczne i rozwój firm w różnych sektorach gospodarki.

W trakcie licznych prezentacji i paneli dyskusyjnych przedstawiciele Milestone Systems oraz partnerzy technologiczni firmy

omówili praktyczne zastosowania dozoru wizyjnego – od ochrony infrastruktury krytycznej, przez inteligentne miasta, po branżę detaliczną.

Program wydarzenia otworzyli **Michał Hillel i Borislava Kenarova** z Milestone Systems, podkreślając znaczenie elastyczności i otwartości platformy Milestone XProtect. Następnie **Kliment Todor**, Dyrektor ds. inżynierii, zaprezentował potencjał otwartej platformy Milestone w budowaniu zintegrowanych ekosystemów bezpieczeństwa.

Sporo emocji wzbudziło wystąpienie **Tanyi Tzigularovej i Wojciecha Grabonia**, którzy pokazali, jak nowoczesne systemy wizyjne wspierają rozwój inteligentnych miast i ochronę infrastruktury. O roli sztucznej inteligencji w branży security mówił z kolei **Barry Norton**, przedstawiając projekt **Hafnia** – inicjatywę Milestone dotyczącą zastosowania generatywnej AI w rozwiązaniach bezpieczeństwa.

W sesji poświęconej analityce wizyjnej **Florian Leibovici** zaprezentował, jak rozwiązania oparte na AI pomagają organizacjom

oszczędzać czas, redukować koszty i zwiększać efektywność operacyjną.

Między wystąpieniami uczestnicy mogli odwiedzić strefę **EXPO**, gdzie swoje rozwiązania prezentowali partnerzy technologiczni Milestone, w tym firmy: **2N, Aicuda Technology, Asura, Axis Communications, Dallmeier, Hanwha Vision, Honeywell, Lenel S2, Mer Group, Navtech Radar, Nedap, Roger, Saimos, Secure Logiq, Senstar i Zenitel**. Przestrzeń networkingowa stała się miejscem wymiany doświadczeń i inspiracji dla całej branży.

Na zakończenie dnia odbyło się **losowanie nagród** wśród uczestników, którzy odwiedzili wszystkie stoiska partnerów. Spotkanie zwieńczył koktajl, podczas którego rozmowy o przyszłości technologii wideo toczyły się już w mniej formalnej atmosferze.

Milestone Technology Day Poland 2025 potwierdził, że przyszłość branży wideo to nie tylko bezpieczeństwo, lecz także inteligentne wykorzystanie danych, które wspierają innowacje, automatyzację i rozwój biznesu w wielu sektorach gospodarki. •



[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!



Światłowód FFT – krótszy dystans, duże możliwości

Choć światłowód zwykle kojarzy się z transmisją na duże odległości, także na krótszych dystansach jego zastosowanie oferuje szerokie możliwości, w tym ochronę terenów. Przykładem takiego rozwiązania jest nowy sterownik Aura Ai-XS firmy Future Fibre Technologies.

Urządzenie wyposażono w dwa kanały o zasięgu 5 km każdy, co pozwala zabezpieczyć perymetrię placu lub parkingu bez konieczności instalowania zasilania w terenie. Ważnym

atutem systemu jest odporność światłowodu na zakłócenia radiowe, magnetyczne oraz wpływ warunków atmosferycznych. Algorytmy sztucznej inteligencji tworzą modele detekcji ograniczające liczbę niepożądanych alarmów. Dzięki temu skuteczność wykrywania przekracza 95%, przy minimalnej liczbie fałszywych alarmów i dokładności lokalizacji sięgającej ± 2 m.

Dla obiektów pozbawionych ogrodzenia dostępny jest wariant Aura Ai-XSB,

który umożliwia zakopanie światłowodu w ziemi i ochronę samego terenu bez stosowania fizycznej bariery.

Integracja systemu z kamerami rozmieszczonymi wzdłuż linii ogrodzenia zwiększa świadomość sytuacyjną i zapewnia wizualną weryfikację alarmów. Z kolei zamknięcie pętli z obu stron obwodu sprawia, że system pozostaje aktywny nawet w przypadku przecięcia światłowodu. •

Integracja VISO SMS z centralami POLON 4000/6000

W nowoczesnych obiektach zarządzanie bezpieczeństwem wymaga nie tylko skutecznych systemów, ale także ich współdziałania i centralizacji. Firma Roger rozwija VISO SMS – platformę umożliwiającą monitorowanie i zarządzanie systemami bezpieczeństwa z jednego miejsca. Kluczowym obszarem jest integracja z systemami przeciwpożarowymi, w tym z centralami pożarowymi POLON 4000 i POLON 6000 firmy POLON-ALFA. Dzięki temu operatorzy zyskują pełną kontrolę nad sytuacją, a podejmowane decyzje są szybsze i zgodne z obowiązującymi procedurami.

Dzięki tej integracji możliwe jest:

- monitorowanie stanów central pożarowych (alarmy, awarie, testy, uszkodzenia),
- wizualizacja czujek i stref pożarowych na mapach obiektu,
- prezentacja zdarzeń w stosie alarmowym z uwzględnieniem priorytetów,

- lokalizacja źródła zagrożenia w czasie rzeczywistym,
- uruchamianie scenariuszy bezpieczeństwa zgodnych z procedurami obowiązującymi w danym obiekcie (powiadomienie służb, uruchamianie sygnalizacji, sterowanie innymi systemami).

Współpraca obu rozwiązań przynosi szereg korzyści dla administratorów, operatorów i właścicieli obiektów, takich jak:

- szybka i trafna reakcja na zagrożenia,
- centralizacja informacji,
- automatyzacja procedur,
- pełny rejestr zdarzeń,
- skalowalność i elastyczność.

Rozwiązanie sprawdza się w służbie zdrowia, przemyśle, administracji i edukacji, zapewniając zgodność z procedurami i efektywne zarządzanie bezpieczeństwem wszędzie tam, gdzie bezpieczeństwo pożarowe ma istotne znaczenie. •



a&s

Najnowsze informacje
z branży security znajdziesz
na portalu **aspolska.pl**



aspolska.pl:

- Twój portal wiedzy i inspiracji
 - Czytaj, odkrywaj, działaj
- Z nami jesteś zawsze na czasie

CZASOPISMO RYNKU SECURITY



Wesołych Świąt

życzy

BCS



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

