04 (52) / 2025

CZASOPISMO RYNKU SECURITY

a&S POLSKA

RAPORT: FACILITY MANAGEMENT A BEZPIECZEŃSTWO

W świecie, gdzie stabilność i odporność obiektów stają się coraz cenniejszą walutą, Facility Management wchodzi w rolę strażnika codziennego bezpieczeństwa.

KTO I DLA KOGO OPRACOWUJE BRANŻOWE NORMY

Norma PN-EN 62676 Systemy dozoru wizyjnego skierowana jest do wszystkich uczestników sektora: producentów, projektantów i użytkowników.

GDY NIE WIADOMO O CO CHODZI...

Ile kosztuje ochrona, mniej więcej wiadomo. Czy jednak wiadomo, ile tak naprawdę kosztować może rezygnacja z niej? Podpowiadamy, może być drogo...

www.aspolska.pl

20 zł
(w tym 8% VAT)

ISSN 2451-5175 05
9 772451 517703

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

a&S POLSKA

Kto za to odpowiada?

Kto odpowiada za to, że każdego dnia, wyruszając do pracy samochodem, korzystając z komunikacji publicznej, robiąc zakupy albo spotykając się ze znajomymi, możemy się czuć bezpiecznie? Jak to się dzieje, że woda nadaje się do picia, działają światła drogowe, a w hotelowym lobby można zjeść śniadanie?

Otóż za ciepłą wodę w kranie, bezpiecznymi ulicami i autobusami odpowiada... Pan. I Pani. I Pan, młody człowieku również. Tak właśnie. Wy, szanowni Czytelnicy, za to odpowiadacie. To od Waszej pracy, na którą składają się czasami bardzo drobne decyzje, czasami wielkie zadania, ale zawsze towarzyszy jej olbrzymia odpowiedzialność, zależy to, że inni ludzie czują się bezpiecznie.

Sklep, galeria handlowa, hotel, ośrodek konferencyjny, miejska biblioteka, muzeum czy oddział szpitalny – każdy z tych obiektów potrzebuje ludzi, którzy odpowiadać będą za zarządzanie nim, jego bezpieczeństwo. A w ostatecznym rozrachunku za doświadczenie (tzw. *customer experience)*, jakie wyniesie klient odwiedzający sklep, muzeum, czy hotel. Między innymi o tym piszemy w artykule *Facility Management a bezpieczeństwo: niewidzialna architektura bezpiecznego obiektu* (s. 12).

Facility management potrzebuje narzędzi. Te zapewnia współczesna technologia. Oczywiście cyfrowa i wspomagana przez algorytmy sztucznej inteligencji. Systemy VMS (str. 18), analiza wideo, integracja kontroli dostępu czy karty wirtualne (*Nowe trendy w systemach kontroli dostępu: od Wieganda do kart wirtualnych*, str. 27) to współcześnie niezbędnik facility managera. Jednak sprzęt i algorytmy działają w konkretnym kontekście. Poznanie tego kontekstu wymaga odpowiedzi na pytania: Co ma być celem dozoru? Jakie ryzyka należy przewidzieć? Kto podejmuje decyzję w przypadku sytuacji kryzysowej? Odpowiedź ułatwi zastosowanie normy PN-EN 62676, która przypomina o tym, określając wymagania projektowe i kryteria oceny instalacji. Więcej na jej temat w artykule *Kto i dla kogo opracował normę PN-EN 62676. Systemy dozoru wizyjnego* na str. 22

To zrozumiałe, że plan ochrony musi uwzględniać funkcje obiektu, natężenie ruchu i obecność w nim osób. To też oczywiste, że lepsze są systemy zintegrowane niż działające każdy z osobna. Ale wiadomo też, że sama integracja nie gwarantuje skuteczności. Kompetencje personelu i jasne procedury decydują o tym, czy system zda egzamin w realnej sytuacji. O tym, m.in. w artykule *Samorządy w pułapce cyfrowego chaosu* (str. 50).

Funkcjonowanie w ramach branży ochrony oznacza nie tylko wyzwania związane z zadaniami stojącymi przed firmami security, ale także te związane z utrzymaniem kadr. Duża rotacja, presja kosztowa i braki kadrowe – to dzisiejsza rzeczywistość w wielu firmach security. Inna rzecz, że każda świadoma zagrożeń organizacja powinna pamiętać o tym, że niełatwo o zachowanie bezpieczeństwa wewnętrznego bez ćwiczeń, procedur i odpowiednich zabezpieczeń technicznych. Dlatego warto zawsze rozważyć współpracę z doświadczonym partnerem. O czym przypomina *Głos branży*, str. 46.

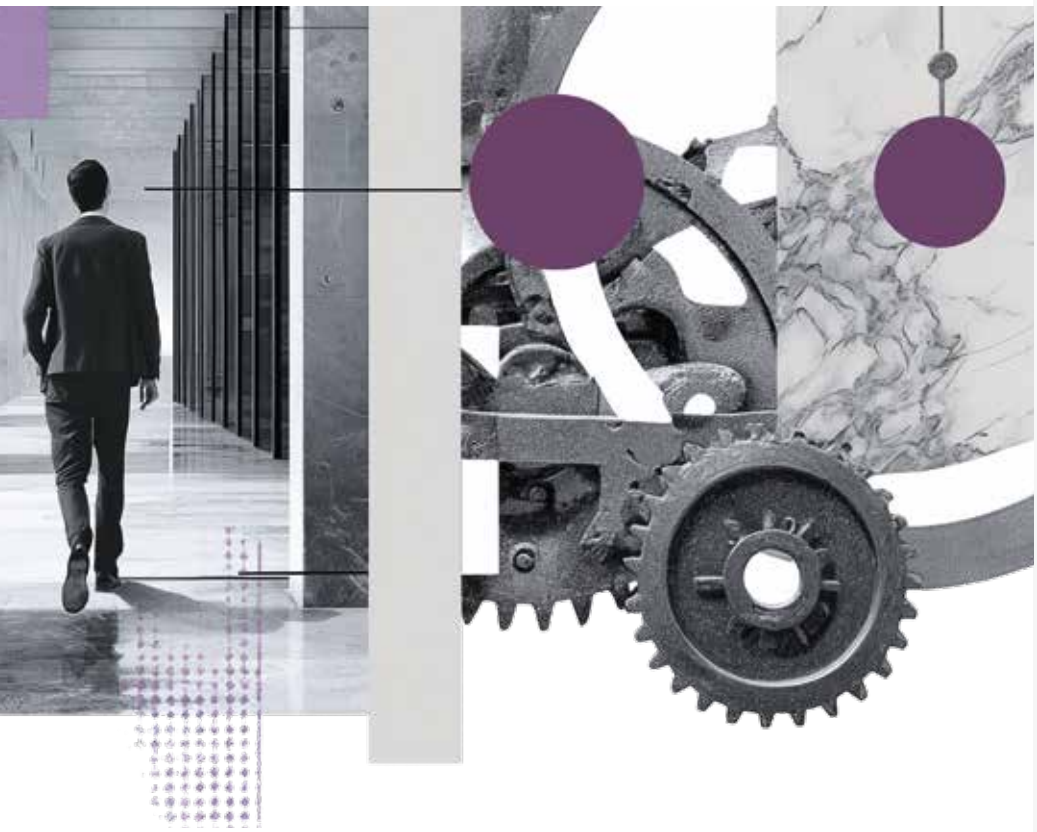
Bezpieczeństwo to proces. Regularne przeglądy, aktualizacja procedur, ćwiczenia i audyty utrzymują systemy w sprawności. Dobrze zaprojektowany system, zgodny z normami i obsługiwany przez przeszkolony personel działa efektywnie. Jeśli zasoby własne nie wystarczają, te zadania warto zlecić profesjonalistom. Projekt, technologia, procedury i ludzie to elementy, które powinny działać syngergicznie. Dla bezpieczeństwa wszystkich osób: Pani i Pana, i tak, tak... Pana też. •

Redakcja

CZASOPISMO RYNKU SECURITY

a&S POLSKA

04 (52) / 2025



Spis treści

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

BCS®

dla profesjonalistów

tworzyMY

Stacja monitoringu z autorskim oprogramowaniem firmy BCS

BCS-F-STATION

• System operacyjny Linux • Procesor Intel Core i7 • Podgląd / odtwarzanie na jednej karcie do 64 kanałów
• Opcjonalnie karta graficzna z 4 wyjściami monitorowymi
• Funkcje: e-Mapa, POS, analizy obrazu z kamer, rozbudowane alarmy
• Współpraca ze wszystkimi rejestratorami i kamerami BCS (ONVIF i obsługa innych marek z dodatkową licencją)
• Integracja: SSWiN - Pulson Alarm, Satel, SSP - Polon Alfa, Siemens oraz Modbus • Zgodność z NDAA

POLSKA MARKA BCS

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

NDAA COMPLIANT

MANUFACTURED IN EU

CZASOPISMO RYNKU SECURITY

a&S POLSKA

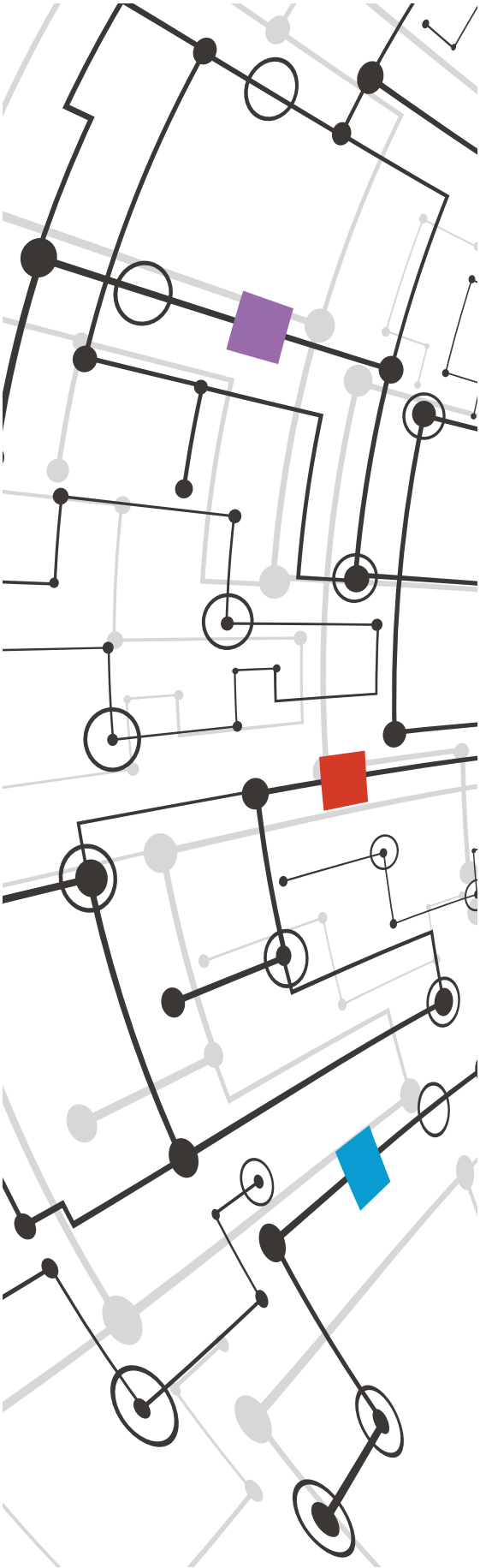
04 (52) / 2025

Spis treści

RYNEK SECURITY

CYBERBEZPIECZEŃSTWO

BEZPIECZEŃSTWO POŻAROWE



Dla firm

Bezpieczny Wodociąg od Orange

orange™ tu jest

Skorzystaj z finansowania w ramach programu „Cyberbezpieczne Wodociągi”

Zwiększ poziom bezpieczeństwa IT i OT w swoim przedsiębiorstwie wodno-kanalizacyjnym dzięki kompleksowej ofercie Orange

Dlaczego warto?

- **Finansowanie do 100% inwestycji – maksymalnie 300 tys. EUR**
- **Wsparcie w uzyskaniu funduszy – pomoc w przygotowaniu wniosku i dokumentacji**
- **Kompleksowe rozwiązania – od przeglądu bezpieczeństwa po wdrożenie systemów ochrony**

Nasza oferta obejmuje:

Przegląd bezpieczeństwa IT i OT

- Analiza mocnych i słabych stron
- Ocena zgodności z normami (ISO 27001, NIS2, ISA/IEC 62443)
- Rekomendacje i plan działań

Wdrożenie przemysłowego systemu IDS

- Monitoring sieci OT i identyfikacja urządzeń
- Wykrywanie zagrożeń i podatności
- Zgodność z regulacjami i standardami

Usługi dodatkowe

- Budowa Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
- Szkolenia z zakresu cyberbezpieczeństwa
- Usługa SOC (Security Operations Center) – monitoring 24/7

Korzyści dla Twojej firmy:

- **Wyższy poziom cyberodporności**
- **Zgodność z regulacjami i standardami bezpieczeństwa**
- **Szybsza reakcja na incydenty**
- **Solidne uzasadnienie inwestycji w cyberbezpieczeństwo**

Więcej na orange.pl

BCS

Funkcjonalności aplikacji BCS Manager

Duża różnorodność rozwiązań security dostępnych na polskim rynku często przyprawia instalatorów i integratorów o ból głowy. Aplikacja BCS Manager to rozwiązanie przeznaczone do obsługi urządzeń różnych producentów, nie tylko marki BCS. Sprawdza się zarówno w przypadku małych instalacji, składających się z kilku kamer, jak i dużych systemów liczących nawet kilkaset kanałów.

Liczba kamer obsługiwanych przez system zależna jest od wydajności komputera, na którym zainstalowana jest aplikacja. Możliwe jest jednoczesne wyświetlenie nawet kilkunastu ekranów podglądu w dowolnym podziale.

Aplikacja może działać w architekturze serwera z nieograniczoną liczbą podłączonych do niego klientów. Ta wersja zawiera m.in. funkcje obsługi kamer rozpoznających tablice rejestracyjne i trasy pojazdów, moduł integracji z systemami WMS lub POS, a także moduł wirtualnych obchodów oraz moduł służący do rejestrowania w pamięci serwera inforamcji o alarmach z urządzeń klienckich.

Ważną cechą, na którą należy zwrócić uwagę podczas tworzenia centrum nadzoru w rozbudowanych obiektach, jest możliwość integracji z wybranymi systemami ppoż. oraz SSWIN wraz z możliwością wizualizacji

alarmów na mapie obiektu. Aplikację można zainstalować zarówno na systemach operacyjnych Windows, jak i na dystrybucjach Linuxa.

Więcej na: **www.bcs.pl**

HIKVISION

Rewolucyjna funkcja AcuSeek w nowej serii rejestratorów Hikvision

Technologia AcuSeek w nowych rejestratorach Hikvision jest funkcją inteligentnego wyszukiwania nagrań opartą na prostym mechanizmie typu „Napisz czego szukasz" (Type it, Seek it). Dzięki tej innowacji użytkownik nie musi już przeszukiwać godzin materiału – wystarczy, że wpisze, czego szuka, a system natychmiast wyświetli odpowiednie fragmenty nagrań.

Funkcja „Napisz czego szukasz" bazuje na wieloskalowych sztucznych sieciach neuronowych i modelu sztucznej inteligencji typu LMM *(Large Multimodal Model)*. Użytkownik może wpisać np. „osoba w czerwonej kurtce", „samochód dostawczy" czy „osoba na spacerze z psem", a system automatycznie przeanalizuje nagrania i wskaże momenty, które spełniają te kryteria. To prawdziwy przełom w szybkim wyszukiwaniu i analizie zdarzeń.

Funkcja AcuSeek wspiera kamery IP wysokiej rozdzielczości i współpracuje z chmurą Hik-Connect, co umożliwia zdalny podgląd z aplikacji mobilnej. To idealne rozwiązanie dla firm, instytucji i użytkowników domowych oczekujących skutecznego monitoringu z inteligentną analizą obrazu.

Więcej na: **www.hikvision.com/pl/**

LINC POLSKA

Nowa kamera bispektralna Dual-Sensor & Dual-Light serii 35 marki Honeywell

Model HC35WMBAR1 wyposażono w technologię inteligentnego podwójnego oświetlenia (Dual-Light – światło białe + IR) zapewniającą kolorowy obraz przez całą dobę. W nocy działa oświetlacz podczerwieni (IR), a po wykryciu obiektu uruchamia się światło białe, by uchwycić szczegóły zdarzenia w kolorze.

Kamera została wyposażona w szereg zaawansowanych funkcji wspierających bezpieczeństwo obiektów:

- panoramiczny obraz 180° dzięki wbudowanym dwóm przetwornikom i obiektywom,
- przetworniki obrazu STARVIS II zapewniające wyjątkową jakość obrazu o dużej szczegółowości w rozdzielczości 4K,
- obraz wizyjny i termowizyjny,
- funkcję Defog poprawiającą jakość obrazu w trudnych warunkach atmosferycznych,
- dwukierunkowe audio (mikrofon i głośnik, transmisja 30 m/69 dB),
- zapis na kartę SD,
- zgodność z ONVIF G/S/T/M, zabezpieczenia HTTPS, filtr IP, uwierzytelnianie Digest, TLS1.2/1.3, szyfrowanie strumieniowe, AES128/256, zamknięte SSH/Telnet, zgodność z PCI-DSS, wbudowany chipset szyfrujący, bezpieczny rozruch,
- wbudowaną analitykę: wykrywanie włamania, podejrzanych osób, zliczanie ludzi, wykrywanie twarzy, przekroczenie linii, zmiana sceny, wykrywanie porzuconego lub brakującego obiektu, mapy ciepła,
- solidna obudowa IK10 z elastycznym montażem, dzięki obrotowi kamery na uchwycie w poziomie 360° i w pionie 90°.

Kamera jest objęta 5-letnią gwarancją producenta, jest idealna do obiektów handlowych, parkingów, magazynów czy stadionów. Więcej na: **www.linc.pl**

RACS 5

roger
ASSA ABLOY

Nowoczesna transformacja bez rewolucji

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

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

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

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

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

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

Experience a safer
and more open world

TP LINK

TP-Link ER706WP-4G – gigabitowy router z Wi-Fi 6 i obsługą dwóch kart SIM

TP-Link wprowadził do oferty nowy model z serii Omada – gigabitowy router ER706WP-4G z obsługą LTE i technologią Wi-Fi 6 oraz dwoma slotami na karty nano SIM.

ER706WP-4G zaprojektowano z myślą o zachowaniu ciągłości pracy w każdej sytuacji. Dzięki dwóm slotom na kartę nano SIM urządzenie zapewnia pełną redundancję – nawet w przypadku awarii głównego połączenia internetowego router automatycznie przełącza się na alternatywne źródło sygnału LTE. Modem LTE Cat6 pozwala uzyskać dostęp do Internetu 4G+ LTE, dzięki czemu zapewnia możliwość backupu sieci w przypadku awarii łącza głównego. Sprawdzi się niezawodnie w biurach, hotelach, placówkach edukacyjnych, magazynach czy halach produkcyjnych – wszędzie tam, gdzie sieć musi działać nieprzerwanie.

Router oferuje dwupasmowe Wi-Fi 6 w standardzie AX3000, zapewniając imponującą przepustowość – do 2402 Mb/s w paśmie 5 GHz oraz 574 Mb/s w paśmie 2,4 GHz. Urządzenie oferuje łącznie 6 gigabitowych portów Ethernet – jeden port SFP WAN/LAN, jeden port WAN oraz cztery porty WAN/LAN zgodne z PoE 802.3at.

Kluczowym elementem rozwiązania jest integracja z platformą Omada SDN. Dzięki centralnemu zarządzaniu w chmurze możliwa jest pełna kontrola dostępu i bezpieczeństwa, a także szybka konfiguracja z poziomu aplikacji mobilnej. Urządzenie stanowi integralną część ekosystemu Omada, gwarantując spójność, elastyczność i wysoki poziom ochrony całej sieci.

Urządzenie zostało objęte 5-letnią gwarancją producenta.

Więcej na: **www.tp-link.com/pl/**

UNICARD

UC 8000 – sterownik kontroli dostępu nowej generacji

Unicard Systems wprowadza na rynek UC 8000 – nowoczesny sterownik polskiej produkcji do kontroli dostępu, zaprojektowany jako centralny element ekosystemu bezpieczeństwa wraz z chmurowym oprogramowaniem KD impero 360. Urządzenie współpracuje także z lokalną platformą UniKD, co daje swobodę wyboru modelu wdrożenia.

UC 8000 wyróżnia się obsługą protokołu OSDP, gotowością do spełnienia wymogów dyrektywy NIS2 i rozporządzenia CER, a także otwartą architekturą, które umożliwia integrację z innymi systemami, w tym ANPR oraz biometrią. Praktycznie nieograniczona pamięć pozwala przechowywać dowolną liczbę uprawnień i rejestracji, a wysoki poziom zabezpieczeń chroni przed nieautoryzowanym dostępem.

Sterownik oferuje zaawansowane funkcje serwisowe: zdalną konfigurację, automatyczne aktualizacje oprogramowania, możliwość przywrócenia stanu fabrycznego *(recovery)*, wizualną prezentację stanu urządzenia oraz zautomatyzowany monitoring pracy w trybie 24/7 w celu szybkiej diagnostyki i napraw. Dzięki temu czas utrzymania systemu jest znacząco skrócony, a ciągłość działania maksymalnie zabezpieczona. Instalacje oparte na UC 8000 wyróżniają się także bardzo wysoką niezawodnością.

UC 8000 jest rozwiązaniem AI ready, skalowalnym i niezawodnym, przygotowanym do pracy w obiektach o najwyższych wymaganiach w zakresie kontroli dostępu oraz bezpieczeństwa.

Więcej na:
https://unicard.pl

W2 POLAND

Nowoczesne sygnalizatory pożarowe serii P8

Do serii P8 należą sygnalizatory: SA-P8 (akustyczny), SO-P8 (optyczny) oraz SAO-P8 (akustyczno-optyczny). Wszystkie wymienione urządzenia mają aktualne dokumenty CNBOP-PIB – Certyfikaty Stałości Właściwości Użytkowych oraz Świadectwa Dopuszczenia.

Urządzenia zostały zaprojektowane z myślą o zastosowaniu w budynkach o zróżnicowanej charakterystyce. Przykładowo, w sygnalizatorach wewnętrznych SA-P8 i SAO-P8 zaimplementowano takie funkcje, jak: możliwość wyboru jednego z 16 wzorów dźwięku, opcję stopniowego narastania jego poziomu, a także jego regulację za pomocą potencjometru. Dzięki temu sygnalizatory te można dostosować do specyfiki konkretnego obiektu, np. poziomu szumów (hałasu) tła.

Sygnalizatory z członem optycznym – zewnętrzny SO-P8 oraz wewnętrzny SAO-P8

– umożliwiają wybór generowanej bryły optycznej (3, 6, 9, 12 m) w obrębie danego urządzenia. Dzięki temu mogę być stosowane zarówno w przestrzeniach o standardowej, jak i większej wysokości montażu (np. hale magazynowe).

Przygotowanie urządzenia do pracy w docelowych warunkach jest bardzo proste – wymaga jedynie zmiany fabrycznych ustawień mikroprzełączników.

Seria sygnalizatorów P8 wyróżnia się możliwością montażu na ścianie lub suficie, wytrzymałą obudową o odporności mechanicznej IK07, szerokim wyborem dostępnych odmian oraz możliwością synchronizacji (pracy w sieci). Urządzenia są również kompatybilne z sygnalizatorami SA-K7N, SA-K5N oraz SAOZ-Pk2.

Więcej na: **www.w2.com.pl**

POLON-ALFA

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!

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

Facility Management a bezpieczeństwo:

niewidzialna architektura bezpiecznego obiektu

Nowoczesne budynki: biurowce i galerie handlowe, obiekty przemysłowe i centra logistyczne nie mogą funkcjonować bez zaplecza zarządzającego ich infrastrukturą. Facility management, choć często niewidoczny dla użytkowników końcowych, pełni dziś jedną z kluczowych funkcji w organizacji codziennego działania oraz zapewnienia bezpieczeństwa w obiektach niemieszkalnych. W czasach rosnących zagrożeń – zarówno fizycznych, jak i cyfrowych – zarządzanie obiektem to już nie tylko konserwacja wind i nadzór nad czystością, ale także aktywne uczestnictwo w systemie ochrony. Jak jedno łączy się z drugim i przed jakimi wyzwaniami stoi obecnie FM?

Adela Prochyra

Od sprzątania do zarządzania ryzykiem

Facility management (FM), czyli zintegrowana obsługa obiektów, przeszło w ostatnim czasie ogromną ewolucję. Dawniej kojarzone przede wszystkim z usługami pomocniczymi, stricte wykonawczymi, głównie z zakresu konserwacji obiektów, dziś staje się złożoną usługą integrującą wiele dziedzin, narzędzi i technologii. Obecnie – w modelowym wariancie – obejmuje ono strategiczne zarządzanie całym cyklem życia nieruchomości: dziennym, miesięcznym bądź kwartalnym i rocznym, uwzględniającym zarówno zmiany pór roku, jak i zmiany zakresu użytkowania – od planowania i utrzymania, po bezpieczeństwo, zarządzanie mediami, optymalizację kosztów utrzymania, aż po finalny komfort użytkownika. W obszarze tego procesu zwykle znajduje się bezpieczeństwo fizyczne i techniczne, którego skuteczne modelowanie stanowi dziś warunek stabilnego funkcjonowania każdego obiektu.

Mówi się coraz częściej o tym, że FM staje się dziś „operacyjnym centrum dowodzenia" – punktem styku pomiędzy administracją obiektu, personelem ochrony, służbami technicznymi i działami IT. W maksymalnym ujęciu może obejmować:

- sprzątanie i konserwację (serwis techniczny),
- administrowanie obiektem (wraz z obiegiem dokumentów),
- zarządzanie odpadami,
- obsługę recepcyjną i logistykę,
- utrzymanie zieleni,
- ochronę fizyczną (personel, patrole, kontrola dostępu),
- zarządzanie systemami CCTV i alarmowymi,
- zarządzanie energią i optymalizację kosztów,
- kontrolę nad przepływem osób i pojazdów,
- procedury reagowania kryzysowego,
- prewencję pożarową i ewakuacyjną,
- nadzór nad podwykonawcami, zarządzanie umowami i dostawcami,
- usługi specjalistyczne, np. deratyzacja,
- doradztwo i wprowadzanie innowacji.

Zwyczajowo fizyczne elementy infrastruktury, np. windy, schody ruchome, okablowanie, wentylację, instalacje, zalicza się do tzw. twardego (*hard*) Facility Management. Natomiast obszar związany z ludźmi i organizacją, np. sprzątanie, obsługa recepcji, catering, rezerwacja przestrzeni konferencyjnych, nazywa się miękkim (*soft*) Facility Management.

Facility Management 4.0: kiedy technologia przejmuje kontrolę

Aby skutecznie koordynować tak różnorodne procesy – od monitoringu bezpieczeństwa, przez optymalizację zużycia mediów, aż po kontakt z użytkownikami – potrzebne są dziś zaawansowane, zintegrowane systemy cyfrowe. Dzisiejsze FM opiera się w coraz większym stopniu na inteligentnych narzędziach, które umożliwiają automatyzację, analizę predykcyjną i bieżące reagowanie w czasie rzeczywistym. Eksperci mówią wręcz o tym, że firmy świadczące usługi FM muszą być poniekąd także firmami IT. Co jest w użyciu? Technologie takie jak Internet rzeczy (IoT), sztuczna inteligencja (AI), uczenie maszynowe, big data oraz platformy BMS (*Building Management Systems*) i CAFM (*Computer-Aided Facility Management*) pozwalają nie tylko na precyzyjne zarządzanie obiektem, lecz również na przewidywanie awarii i natychmiastowe reagowanie, optymalizację zużycia energii i podnoszenie poziomu bezpieczeństwa.

W praktyce oznacza to obecność w budynkach takich rozwiązań, jak czujniki temperatury, dymu, ruchu, wilgotności czy obecności, które automatycznie dostosowują parametry pracy systemów HVAC, oświetlenia czy zabezpieczeń. Równie istotne są inteligentne systemy zarządzania energią – szczególnie w połączeniu z odnawialnymi źródłami, takimi jak fotowoltaika

FACILITY MANAGEMENT to dziedzina naukowa koncentrująca się na nowoczesnym podejściu do zarządzania procesami wspierającymi funkcjonowanie organizacji, które odbywają się w budynkach niemieszkalnych.

Termin ten wywodzi się ze Stanów Zjednoczonych i w zależności od kontekstu może być różnie interpretowany – w przypadku nieruchomości oznacza „zarządzanie udogodnieniami", natomiast w odniesieniu do organizacji odnosi się do „zarządzania procesami pomocniczymi".

Po raz pierwszy został użyty w latach 60. przez Rossa Perota, byłego sprzedawcę w IBM i założyciela Electronic Data Systems, w odniesieniu do zarządzania systemami i sieciami IT, ale jego definicja szybko się rozszerzyła.

i magazyny energii – które wspierają nie tylko redukcję kosztów, ale również odporność infrastruktury na zakłócenia w dostawach mediów. W obszarze bezpieczeństwa fizycznego na pierwszy plan wysuwają się systemy CCTV wspierane przez AI, zdolne do analizowania obrazu w czasie rzeczywistym i wykrywania zagrożeń, zanim dojdzie do incydentu. Z kolei systemy kontroli dostępu integrujące dane z kart zbliżeniowych, kodów QR, biometrii czy rejestracji pojazdów pozwalają na pełną kontrolę przepływu osób i pojazdów na terenie obiektu.

Prawdziwy potencjał tych technologii ujawnia się wtedy, gdy zostaną one zintegrowane w spójny system. Takie rozwiązania tworzą cyfrowy ekosystem zarządzania budynkiem – łączący obszary tzw. hard FM i soft FM w ramach jednej platformy. Coraz więcej rozwiązań umożliwia obsługę wielu procesów – od serwisu technicznego, przez harmonogramy przeglądów, aż po komunikację z najemcami – w jednym interfejsie. Poszczególne rozwiązanie software'owe dla FM oferują rzecz jasna różne kombinacje i możliwości, ale nie można zapomnieć, że samo oprogramowanie jest tylko częścią procesu zachowania ciągłości biznesu – w modelowym wydaniu zaprojektowanego kompleksowo i z wyprzedzeniem. Składają się na niego szczegółowo opracowane procedury postępowania w konkretnych przypadkach, np. zalania czy awarii zasilania. Należy też wziąć poprawkę na to, że potrzeby w różnych sektorach będą różne i rozwiązania FM będą projektowane inaczej np. dla lotnisk, a inaczej dla biurowca.

FM na wyciągnięcie ręki: mobilność i użytkownik w centrum

Jednym z ostatnich trendów w FM jest przeniesienie ciężaru obsługi z „back office'u" na użytkownika końcowego – rozumianego zarówno jako podwykonawcę, czyli osobę odpowiedzialną za sprzątanie, jak i klienta danego obiektu. Nowoczesne obiekty wyposażone są dziś również w interfejsy użytkownika – od bardzo prostych rozwiązań, jak kody QR po aplikacje mobilne czy portale online – które umożliwiają szybką, intuicyjną interakcję z infrastrukturą budynku. Za pomocą jednego interfejsu użytkownicy mogą dziś:

- **zgłaszać** usterki techniczne i śledzić status ich realizacji,
- **rezerwować** sale konferencyjne i strefy wspólne w czasie rzeczywistym,
- **otrzymywać powiadomienia** o planowanych pracach serwisowych,
- **monitorować** zużycie mediów (np. w modelach rozliczeń podnajemców),
- **zamawiać** dodatkowe usługi (np. sprzątanie, dostęp dla gościa),
- **kontaktować się bezpośrednio** z serwisem technicznym lub recepcją.

Dla zarządców obiektu oznacza to zupełnie nowe możliwości: automatyczne delegowanie zadań, dostęp do danych operacyjnych w czasie rzeczywistym, lepszą kontrolę nad efektywnością pracy zespołów terenowych oraz bardziej przejrzyste raportowanie. Dla użytkowników – wzrost komfortu, poczucie sprawczości i przejrzystość usług, co przekłada się na pozytywne doświadczenia z użytkowania przestrzeni. W efekcie Facility Management przestaje być niewidzialną infrastrukturą w tle, a staje się cyfrową, aktywną usługą, dostosowaną do wymagań współczesnych użytkowników i dynamicznego, często hybrydowego modelu pracy.

Systemy zabezpieczeń, czyli cyfrowy pancerz budynku

Gdzie w tym wszystkim znajduje się bezpieczeństwo? To dziś jeden z filarów nowoczesnego Facility Management – nie tylko jako część operacyjnej obsługi obiektu, lecz także jako istotny element strategii organizacyjnej. Niezależnie od tego, czy mówimy o centrum danych, zakładzie przemysłowym czy przestrzeni

biurowej, bezpieczeństwo musi być zaprojektowane systemowo i strategicznie.

Współczesne systemy zabezpieczeń coraz częściej działają w modelu chmurowym, operując na ogromnych zbiorach danych – zarówno firmowych, jak i osobowych. Zbierają informacje o dostępie do przestrzeni, aktywności użytkowników, działaniu urządzeń i reakcjach systemów. Oznacza to, że granica między bezpieczeństwem fizycznym a cyfrowym bardzo się zatarła, a skuteczne zarządzanie tym obszarem wymaga myślenia holistycznego.

W skład cyfrowej infrastruktury bezpieczeństwa wchodzą dziś m.in.:

- **monitoring wizyjny (CCTV)** z analizą obrazu w czasie rzeczywistym i wspomaganiem przez AI,
- **systemy kontroli dostępu** (biometria, karty RFID, mobilne identyfikatory),
- **czujniki środowiskowe** (dym, temperatura, wycieki, wibracje),
- **zintegrowane platformy PSIM** (*Physical Security Information Management*), które konsolidują dane z różnych źródeł i umożliwiają szybką reakcję,
- **infrastruktura IT:** firewalle, systemy detekcji włamań, monitoring sieci i segmentacja zasobów cyfrowych.

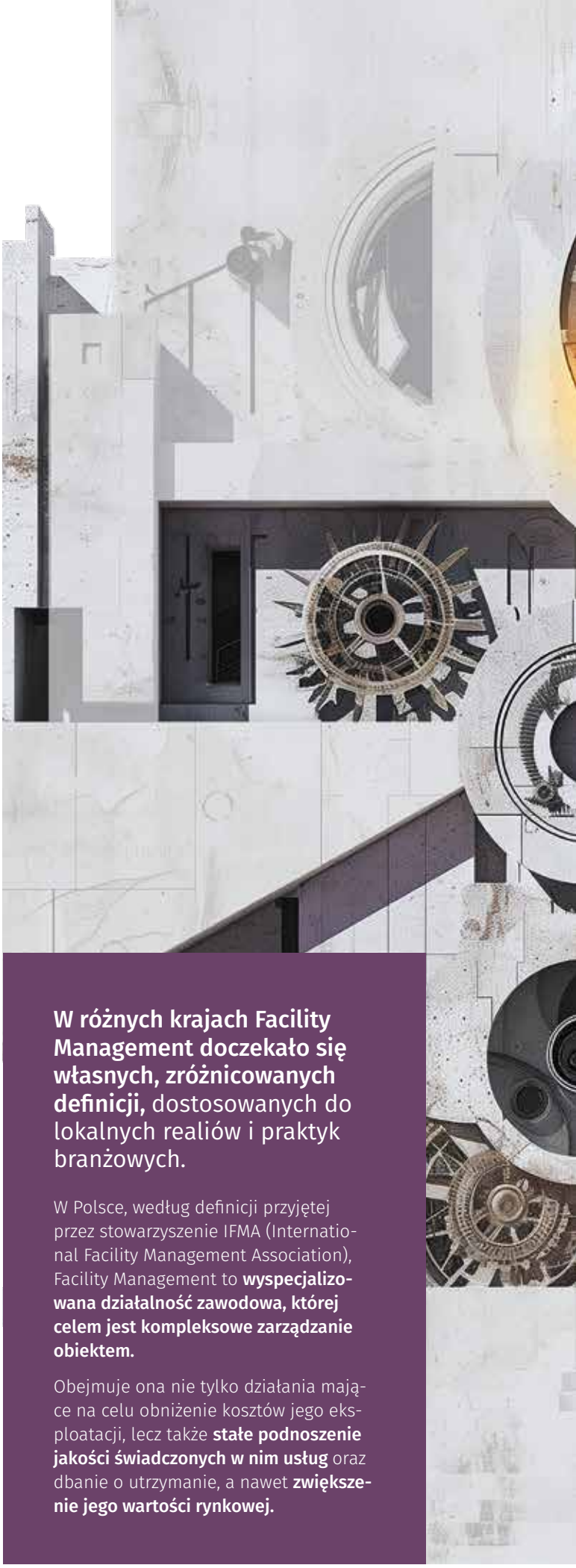
W tym kontekście rola facility managera zmienia się radykalnie. Nie jest on już tylko „technicznym gospodarzem" obiektu, ale staje się aktywnym członkiem zespołu ds. zarządzania ryzykiem, odpowiedzialnym za wdrażanie polityk bezpieczeństwa – zarówno fizycznego, jak i operacyjnego. Jego zadania nie ograniczają się do wyboru dostawcy systemu alarmowego czy koordynacji ochrony fizycznej. Coraz częściej to właśnie FM odpowiada za:

- **tworzenie i aktualizację planów awaryjnych** (*Business Continuity Plan*),
- **przygotowanie infrastruktury** na zdarzenia ekstremalne (pożary, awarie, akty wandalizmu, sabotaż),
- **ocenę ryzyka** przy wdrażaniu nowych technologii lub zmianie przeznaczenia obiektu,
- **monitorowanie zgodności** z wymaganiami certyfikacyjnymi, takimi jak ISO 27001 (bezpieczeństwo informacji), ISO 41001 (zarządzanie FM) czy TAPA (dla sektora logistycznego i transportowego).

Znaczenie tych działań rośnie szczególnie w przypadku infrastruktury krytycznej – centrów danych, hubów logistycznych, zakładów produkcyjnych czy placówek medycznych – gdzie każda minuta przestoju może oznaczać realne straty finansowe lub zagrożenie życia i zdrowia.

Wyzwania i perspektywy współczesnego Facility Management

Jednym z największych wyzwań stojącym przed branżą FM jest dziś pogodzenie rosnących oczekiwań dotyczących efektywności operacyjnej z jednoczesną presją kosztową oraz wymogami prawnymi i środowiskowymi. Transformacja energetyczna i regulacje w obszarze ESG powodują, że zarządzanie obiektami nie może ograniczać się wyłącznie do utrzymania bieżącej funkcjonalności – musi aktywnie wspierać strategię zrównoważonego rozwoju organizacji. Wymaga to wdrażania rozwiązań minimalizujących



W różnych krajach Facility Management doczekało się własnych, zróżnicowanych definicji, dostosowanych do lokalnych realiów i praktyk branżowych.

W Polsce, według definicji przyjętej przez stowarzyszenie IFMA (International Facility Management Association), Facility Management to **wyspecjalizowana działalność zawodowa, której celem jest kompleksowe zarządzanie obiektem.**

Obejmuje ona nie tylko działania mające na celu obniżenie kosztów jego eksploatacji, lecz także **stałe podnoszenie jakości świadczonych w nim usług** oraz dbanie o utrzymanie, a nawet **zwiększenie jego wartości rynkowej.**

zużycie energii i wody, redukujących emisje CO_2, wspierających gospodarkę obiegu zamkniętego czy certyfikację w standardach takich jak BREEAM, LEED czy WELL. To z kolei generuje potrzebę inwestycji w nowoczesne systemy zarządzania energią i integrację z odnawialnymi źródłami, co nie zawsze jest łatwe w kontekście kosztów początkowych i złożoności projektowej.

Drugim istotnym wyzwaniem jest rosnąca cyfryzacja. Facility Management staje się obszarem silnie zależnym od danych, a integracja wielu systemów – od BMS i CCTV, przez systemy kontroli dostępu, aż po narzędzia CAFM – wymaga wysokiego poziomu kompetencji IT. Równocześnie pojawia się ryzyko związane z cyberbezpieczeństwem, które coraz częściej dotyczy także infrastruktury krytycznej. Facility managerzy muszą zatem nie tylko rozumieć działanie systemów technicznych, ale również aktywnie uczestniczyć w procesach zarządzania ryzykiem cyfrowym i ochroną danych.

Nie mniej istotne jest wyzwanie kadrowe. Branża FM zmaga się z deficytem specjalistów łączących wiedzę techniczną z kompetencjami analitycznymi, organizacyjnymi i cyfrowymi. Nowoczesny facility manager nie jest już tylko administratorem budynku, lecz także koordynatorem procesów, analitykiem danych i partnerem biznesowym zarządów firm. To powoduje konieczność ciągłego podnoszenia kwalifikacji oraz adaptacji do zmieniających się realiów rynku pracy, w tym elastycznych form zatrudnienia i hybrydowych modeli świadczenia usług.

Perspektywy rozwoju FM są jednak bardzo obiecujące. Cyfryzacja i wykorzystanie sztucznej inteligencji otwierają drogę do predykcyjnego zarządzania budynkami, w którym systemy nie tylko rejestrują zdarzenia, ale również przewidują awarie, planują serwis i optymalizują zużycie zasobów. Inteligentne budynki będą reagować na zachowania użytkowników w czasie rzeczywistym, a Facility Management stanie się centrum integrującym bezpieczeństwo, komfort pracy, efektywność energetyczną i strategię ESG w jednym spójnym ekosystemie.

Coraz większe znaczenie będzie mieć także rola FM w budowaniu odporności biznesu *(Business Resilience)*. W obliczu globalnych wyzwań – od zmian klimatycznych i przerw w dostawach energii, przez rosnące ryzyko cyberataków, aż po zagrożenia geopolityczne – zarządzanie obiektami nie będzie już tylko wsparciem operacyjnym, lecz także kluczowym elementem strategii organizacyjnej.

Podsumowując, FM przyszłości to dziedzina multidyscyplinarna, łącząca technologię, bezpieczeństwo, zrównoważony rozwój i doświadczenie użytkownika. Ci, którzy potrafią spojrzeć na Facility Management nie tylko jako na obsługę infrastruktury, ale także jako strategiczną inwestycję w stabilność i konkurencyjność biznesu, zyskają przewagę, której nie da się łatwo skopiować. Co więcej, w świecie, gdzie stabilność i odporność obiektów stają się coraz cenniejszą walutą, Facility Management wchodzi w rolę strażnika codziennego bezpieczeństwa, choć często działa w cieniu. Właściwie zarządzane bezpieczeństwo to dziś nie wydatek, lecz inwestycja: w reputację, ciągłość działania, spokój użytkowników i odporność biznesu. Wszystko wskazuje na to, że rola FM w tym kontekście w najbliższym czasie będzie tylko rosnąć. A ci, którzy potraktują bezpieczeństwo jako integralną część zarządzania nieruchomością, zyskają przewagę konkurencyjną daleko wykraczającą poza tabelki w Excelu. •

Adela Prochyra
redaktorka „a&s Polska"

System VMS jako kręgosłup bezpieczeństwa w nowoczesnym zarządzaniu obiektami

Współczesny Facility Management to znacznie więcej niż utrzymanie techniczne budynków. To również zawiła gra danych, technologii i automatyzacji, które są integralnymi elementami bezpieczeństwa. Co ważniejsze – sprawiają, że ludzie czują się komfortowo, dzięki wysokiej jakości i efektywności operacyjnej.

Piotr Kołodziejczak

Facility Management to skomplikowany proces, który wymaga połączenia różnych systemów – od monitoringu wizyjnego, przez kontrolę dostępu, aż po zarządzanie alarmami, windami czy HVAC.

Nowoczesny Facility Management

Jednym z filarów tego podejścia są nowoczesne systemy VMS *(Video Management System)*. Są to platformy zarządzania materiałem wizyjnym, które stają się sercem działań ochronnych i operacyjnych w obiektach. Wychodząc naprzeciw oczekiwaniom klientów, Hikvision stworzyło platformę HikCentral Professional, która pozwala na centralne zarządzanie wszystkimi procesami. Niezależnie od tego, czy zarządzasz biurowcem, halą produkcyjną, czy kompleksem logistycznym – wszystko masz pod kontrolą z jednego miejsca. HikCentral Professional to coś więcej niż tylko podstawowe zarządzanie systemami w obiekcie.

Zarządzanie z jednego miejsca

Wiodące systemy VMS, takie jak HikCentral Professional, przeszły ewolucję od klasycznych rejestratorów NVR do inteligentnych platform analitycznych i zarządczych. Dziś nie tylko umożliwiają podgląd i archiwizację obrazu z kamer IP, ale też integrują systemy:

- kontroli dostępu (KD),
- alarmowe (SSWiN, SAP),
- rozpoznawania tablic rejestracyjnych (ANPR),
- ochrony perymetrycznej.

Co możemy zyskać, korzystając z HikCentral Professional w zarządzaniu obiektami? Po pierwsze, pełną kontrolę nad bezpieczeństwem. Integracja kamer z czujkami ruchu, czytnikami kontroli dostępu czy systemami przeciwpożarowymi pozwala operatorom reagować na sytuacje w czasie

rzeczywistym, ponieważ widzi on wszystko na jednym ekranie.

Po drugie, zarządzanie dostępem. HikCentral Professional z systemem kontroli dostępu umożliwia kontrolę, kto wchodzi do budynku i z niego wychodzi. Niewątpliwą zaletą jest możliwość zdalnego zarządzania obiektem. Nowoczesne systemy VMS, takie jak HikCentral Professional, oferują zarządzanie z poziomu aplikacji mobilnych i powiadomienia w czasie rzeczywistym.

Kolejną kwestią jest automatyzacja parkingów i logistyki. System rozpoznawania tablic rejestracyjnych pojazdów przyspiesza proces zarządzania parkingiem i prowadzenia ewidencji. Jest to szczególnie istotne w parkach logistycznych, hotelach czy kompleksach biurowych.

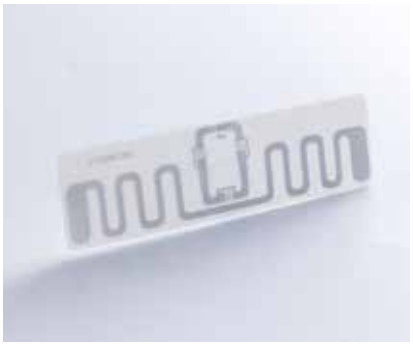
HikCentral Professional – centrum decyzji i kontroli w facility management

HikCentral Professional w praktyce staje się takim narzędziem analitycznym, które pomaga podejmować zarówno szybkie decyzje operacyjne, jak i przygotować długoterminowe plany. Co ciekawe, zdalny dostęp, elastyczność oraz możliwość skalowania to cechy, które naprawdę go wyróżniają. Obecnie system może pracować w chmurze lub na lokalnej infrastrukturze IP. Jest to łatwe i dogodne rozwiązanie. Kontrola nad pracą systemu jest możliwa z poziomu przeglądarki internetowej, bez zbędnych komplikacji.

Czy systemy zarządzania materiałem wizyjnym VMS stały się już koniecznością w zarządzaniu nowoczesnymi obiektami? Wygląda na to, że tak. Bez względu na to, czy mówimy o jednym budynku, czy o sieci placówek – dobrze wdrożony system VMS oszczędza czas i pieniądze oraz przede wszystkim zapewnia bezpieczeństwo. Dzięki modułowej budowie i otwartej architekturze (API/SDK) system można łatwo dostosować do potrzeb różnych obiektów – od biur po zakłady przemysłowe. Jeśli szukasz platformy, która zbierze wszystkie te funkcje w jednym miejscu, HikCentral Professional jest świetnym wyborem, ponieważ dostosowuje się do potrzeb obiektu. •

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

Cyfrowe bezpieczeństwo i efektywność – jak RFID wspiera hotele



Nowoczesne hotele to dziś nie tylko komfort i design – to także precyzyjnie zorganizowane zaplecze operacyjne, które musi działać sprawnie, bezbłędnie i bezpiecznie.

Rosnące koszty, rotacja pracowników oraz coraz większe oczekiwania gości powodują, że coraz częściej hotelarze sięgają po technologię RFID. Rozwiązanie umożliwia automatyczną identyfikację przedmiotów, ludzi i procesów, stając się środkiem do zwiększenia efektywności w niemal każdej strefie obiektu.

Rozwiązania hotelowe RFID stanowią prawdziwy postęp technologiczny, nie tylko optymalizując dostęp do pokoi, ale także ułatwiając płatności bezgotówkowe na terenie hotelu. RFID stanowi zatem kluczową innowację w nowoczesnym hotelarstwie.

– Dzięki technologii RFID wiele hotelowych procesów staje się niemal niewidocznych dla gości. Szybsza obsługa, brak zbędnych formalności i możliwość wygodnego korzystania z udogodnień sprawiają, że pobyt odbierany jest jako bardziej profesjonalny i komfortowy. A to bezpośrednio przekłada się na większą satysfakcję gości i ich chęć do ponownego wyboru tak zarządzanego obiektu – mówi Robert Głażewski, Business Unit Director z Checkpoint Systems Polska.

Coraz popularniejsze staje się też wykorzystanie RFID w zarządzaniu hotelowymi tekstyliami – od pościeli i ręczników po obrusy i szlafroki. Zamiast ręcznego liczenia zasobów pralnia może automatycznie odczytać, ile sztuk trafiło do czyszczenia, i które z nich należą do danego obiektu. Minimalizuje to ryzyko pomyłek. Co więcej, dzięki identyfikowalności w czasie rzeczywistym obiekt zyskuje pełną kontrolę nad przepływem zasobów – zarówno wewnątrz hotelu, jak i przy jego granicach. RFID może być bowiem zintegrowane z systemem bramek antykradzieżowych i czujników, tworząc spójny ekosystem, który zapobiega wynoszeniu oznaczonych przedmiotów poza wyznaczoną strefę. Dodatkowo RFID pozwala hotelarzom planować zakupy i dostawy z uwzględnieniem realnego zużycia i bieżących potrzeb.

RFID wspiera także zarządzanie kuchnią hotelową, a to przecież jedno z najbardziej wrażliwych operacyjnie miejsc w całym obiekcie. Dzięki oznaczeniu pojemników wielokrotnego użytku możliwe jest kontrolowanie ich obiegu, szybsza obsługa dostaw oraz dokładniejszy monitoring dat przydatności. Technologia pozwala też ograniczyć błędy w komunikacji pomiędzy zapleczem gastronomicznym a obsługą.

– W branży hotelarskiej szczególnie ważna jest logistyka zaplecza gastronomicznego. Tu nie ma miejsca na pomyłki. Właśnie dlatego coraz więcej hoteli sięga po etykiety RFID odporne na wilgoć, wysoką temperaturę czy mikrofale. Nasze rozwiązania, takie jak inlay Chinook, umożliwiają skuteczne śledzenie opakowań, rotację zasobów i optymalizację procesów kuchennych – dodaje Robert Głażewski.

Z punktu widzenia zarządzania całym obiektem RFID staje się narzędziem wspierającym nie tylko bezpieczeństwo i automatyzację, ale też zrównoważony rozwój. Umożliwia precyzyjne monitorowanie zasobów, ogranicza marnotrawstwo i pozwala podejmować decyzje w oparciu o twarde dane. To dziś wartość równie ważna, jak komfort gości. Inwestycja w rozwiązania RFID wprost przekłada się na niższe koszty zarządzania obiektem, pozwalając precyzyjnie mierzyć dostępne zasoby, wyeliminować zbędne zamówienia, jak również wyraźnie ograniczyć straty. Dzięki temu koszt wdrożenia nowoczesnego systemu RFID zwraca się nawiązką. •

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

ALNET SYSTEMS

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

www.alnetsystems.com

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

Stosowanie norm jest – co da zasady – dobrowolne. Dlatego opracowuje je branża w zasadzie dla samej siebie. Wieloczęściowa norma PN-EN 62676 skierowana jest do wszystkich uczestników branży systemów dozoru wizyjnego: producentów urządzeń i oprogramowania, projektantów i użytkowników.

Waldemar Więckowski

Oczywiście, nie każda jej część w jednakowym stopniu dotyczy każdej firmy i każdego fachowca świadczącego usługi. Część z nich dotyczy głównie producentów, a część głównie użytkowników. Zabawnym paradoksem może wydać się fakt, że (niektórzy) producenci – sami nie stosując dotyczącej ich części normy – „pouczają" projektantów i użytkowników, że powinni stosować tę część, która ich dotyczy.

Normy opracowuje branża

Wielu uczestników branży sądzi, że normy piszą organizacje normalizacyjne, np. IEC, CENELEC czy w kraju PKN. Skrajnym przejawem tej niewiedzy są formułowane przez uczestników branż zarzuty wobec PKN, że nie publikuje lub nie tłumaczy norm, które są obecne w obiegu europejskim bądź światowym. Tymczasem, organizacje normalizacyjne stanowią „jedynie" formalnoorganizacyjną strukturę normalizacji, w ramach której zainteresowani uczestnicy poszczególnych branż (producenci, projektanci, integratorzy systemów, użytkownicy itd.) opracowują własne i tłumaczą normy międzynarodowe. Dobrowolność normalizacji kojarzy się przede wszystkim z dobrowolnością stosowania norm, ale równie istotna jest dobrowolność udziału w opracowywaniu norm. Dlatego, jeśli w jakiejś branży nie powstają własne normy i/lub nie są tłumaczone normy międzynarodowe, oznacza to ni mniej, ni więcej tyle, że ta branża nie widzi takiej potrzeby.

Nomy to dokumenty techniczne, a nie przepisy prawa

Niektórzy uczestnicy branży zabezpieczeń – również ci o międzynarodowym zakresie działalności – traktują normy techniczne jak przepisy prawa, funkcjonujące na takich samych zasadach, jak ustawy i rozporządzenia. Nic bardziej mylnego. Dobrowolny system normalizacji oznacza, że niestosowanie normy nie jest naruszeniem prawa (i nie podlega karze). W systemie dobrowolnej normalizacji podstawą do określenia cech dostarczanego produktu nie jest norma, ale umowa między dostawcą a odbiorcą. I choć strony umowy nie mają obowiązku odniesienia się w niej do norm, to gdy to uczynią, zachodzi znaczne jej uproszczenie. Wykazanie zgodności z normą może być okolicznością sprzyjającą korzystnemu rozstrzygnięciu w ew. sporze.

Normy dotyczące ochrony technicznej a NIS 2

Normy z branży zabezpieczeń (systemów alarmowych), czyli PN-EN 50131 (SSWiN), PN-EN 62676 (systemy dozoru wizyjnego) oraz PN-EN 60839-11 (elektroniczne systemy kontroli dostępu) nie znalazły się wśród norm powołanych w dyrektywie NIS 2. Nie powołuje się na nie również Ustawa o krajowym systemie cyberbezpieczeństwa. Jednakże, jak zauważył jeden z producentów systemów zabezpieczeń, zgodność ochrony technicznej danej organizacji z normami może znacząco podnieść skuteczność ochrony, co jest istotne w kontekście zgodności tej organizacji z wymaganiami NIS 2. Przy czym zgodność z normami ochrony technicznej nie dotyczy tylko urządzeń i oprogramowania, ale także projektowania i instalacji systemów. Przywołanym przykładem właściwego projektowania lokalizacji i doboru ogniskowej kamery jest uwzględnienie kryteriów związanych z celem dozorowania np. „Wytycznych DORI", które – wg niego – zdefiniowano w normie PN-EN 62676-4:2015-06.

Norma PN-EN 62676-4:2015-06

Ta część normy zawiera wytyczne stosowania systemów dozoru wizyjnego i jest przewodnikiem po procesie ich planowania i projektowania. Dotyczy więc głównie użytkowników (inwestorów) i projektantów.

Jedną z głównych przyczyn niepowodzenia w działaniu systemów dozoru wizyjnego jest to, że ich użytkownicy (inwestorzy) i projektanci nie mają wyraźnie określonego zamysłu co do celu dozoru realizowanego za pomocą każdej kamery w instalacji systemu. Z tego powodu, niemożliwe jest określenie wymagań dotyczących poziomu szczegółowości obrazu dostarczanego przez daną kamerę. Jest to prawdopodobnie powszechny problem, skoro napisano o tym w normie wprost (w wytycznych określania parametrów VSS). Jak zauważa wspomniany wyżej producent systemów zabezpieczeń, nawet doskonałej jakości i bardzo wysokiej rozdzielczości kamera nie spełni swojego zadania, jeśli przy projektowaniu nie uwzględniono celu prowadzenia dozoru wizyjnego. Dlatego adresatami tej uwagi są nie tyle projektanci, ale przede wszystkim użytkownicy (inwestorzy), jako że to oni

Ilustracje: freepik

określają wymagania użytkowe na system (w tym cele prowadzenia dozoru wizyjnego), determinując tym samym rozwiązania projektowe.

„Wytyczne DORI" a cele prowadzenia dozoru wizyjnego

Termin „Wytyczne/Zasięgi DORI" nie występuje w normie PN-EN 62676-4:2015-06. Nie ma go też w pozostałych częściach normy PN-EN 62676. Występuje natomiast w kartach katalogowych kamer na tyle powszechnie, że warto bliżej się temu przyjrzeć. A ponieważ nie jest to termin znormalizowany, w dalszej części artykułu określenia „Wytyczne/Zasięgi DORI" ujęte są w cudzysłów.

Gwoli ścisłości: skrót (?) MDORII pojawiał się w wewnętrznych prezentacjach Grupy Roboczej IEC, która opracowała przedmiotową normę, ale na żadnym etapie nie w jej treści. (Przykład pokazano na ilustracji MDORII w prezentacji IEC).

Te osoby, których brak „Wytycznych/Zasięgów DORI" nie zniechęci do normy i pójdą tropem rozwinięcia skrótu DORI – Detekcja, Obserwacja, Rozpoznanie, Identyfikacja – łatwo odnajdą w niej te terminy. Wspólnie z jeszcze dwoma innymi terminami – Inspekcja i Monitorowanie (Kontrola tłumu) – tworzą one wspólną całość opisaną jako „Pole widzenia – wielkość obiektu". Jak czytamy w normie: Wielkość przedmiotu (obiektu) na ekranie wyświetlacza powinna pozostawać w związku z zadaniami operatora (...).. Zdefiniowano także sześć, a nie cztery, zadania operatora, dla każdego z nich określając precyzyjnie poziom szczegółowości obrazu (minimalną liczbę pikseli obrazu przypadającą na mm obiektu). Zadanie monitorowania najłagodniejsze wymagania na poziom szczegółowości obrazu, zaś Inspekcji (w krajowej praktyce nazywanej Identyfikacją procesową) – najostrzejsze. Ustawiając zadania w kolejności od narzucającego wymagania najłagodniejsze do najsurowszych, otrzymamy: Monitorowanie, Detekcja, Obserwacja, Rozpoznanie, Identyfikacja i Inspekcja – czyli MDORII.

Dlaczego DORI, a nie MDORII?

Skoro w normie zdefiniowano sześć zadań operatora systemu dozoru wizyjnego (których nigdzie w normie nie określono skrótem MDORII), to dlaczego producenci kamer upodobali sobie powoływanie się wyłącznie na cztery zadania (pomijając skrajne), dla których podają wartości liczbowe nazywane „Zasięgami DORI"? Dociekanie, dlaczego, tak naprawdę nie ma praktycznego znaczenia. Niektórzy producenci kamer wyjaśniają, że są to najczęściej realizowane zadania w rzeczywistych instalacjach VSS. To spostrzeżenie jest trafne i można je przyjąć. Praktyczne znaczenie ma natomiast sposób, w jaki określane są owe „Zasięgi DORI".

„Zasięgi DORI", czyli diabeł tkwi w szczegółach

Bezrefleksyjne wykorzystanie w projekcie instalacji VSS „Zasięgów DORI", podawanych w danych katalogowych, może

MDORII w prezentacji IEC

(1) Ustawienie jakości obrazu w zależności od celu prowadzenia dozoru wizyjnego (w tytule slajdu) oraz (2) decyzja o wyborze celu prowadzenia dozoru dla każdego punktu kamerowego (w czerwonej ramce).

M **Monitor**. Do monitorowania lub kontroli tłumu cel powinien zajmować nie mniej niż 5% wysokości obrazu (lub mieć więcej niż 80 mm na piksel) – 12 pikseli/m

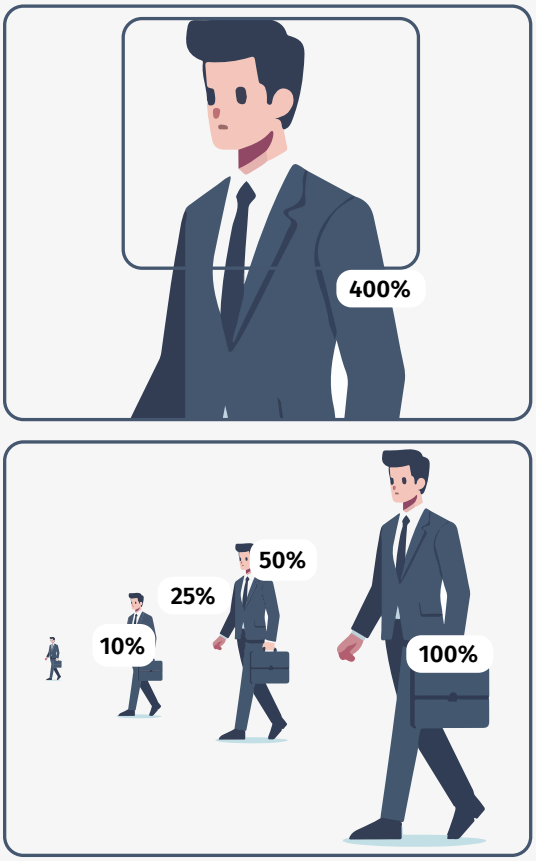
D **Detect**. Do wykrycia celu cel powinien zajmować nie mniej niż 10% wysokości obrazu (lub mieć więcej niż 40 mm na piksel) – 25 pikseli/m

O **Observe**. Do obserwacji celu cel powinien zajmować 25% wysokości obrazu (lub mieć więcej niż 16 mm na piksel) – 62 piksele/m

R **Recognize**. Do rozpoznania celu cel powinien zajmować nie mniej niż 50% wysokości obrazu (lub mieć więcej niż 8 mm na piksel) – 125 pikseli/m

I **Identify**. Do identyfikacji celu cel powinien zajmować nie mniej niż 100% wysokości obrazu (lub mieć więcej niż 4 mm na piksel) – 250 pikseli/m

I **Inspect**. Do inspekcji celu cel powinien zajmować nie mniej niż 400% wysokości obrazu (lub mieć więcej niż 1 mm na piksel) – 1000 pikseli/m



Norma rozróżnia dwa rodzaje rozdzielczości:
• wizualną, która jest miarą zdolności kamery (lub systemów wizyjnych) do reprodukcji szczegółów oryginalnej sceny;
• formatu obrazu będącą opisem rozmiaru cyfrowego obrazu w pikselach (np. 720P, 1080P, 640 × 480), pikselach na cal lub w liczbie pikseli ramki obrazu.

uniemożliwiać realizację wyznaczonych przez użytkownika celów prowadzenia dozoru wizyjnego. Przypomnijmy, że chodzi o zasięg pola widzenia kamery, w którym operator może realizować dany cel (np. identyfikację obiektu).

Niektórzy producenci kamer zamieszczają uwagę, że podane wielkości zasięgów dają ogólne pojęcie o możliwościach kamery i że zostały wyliczone na bazie parametrów przetwornika obrazu. Wielu użytkownikom i (niestety) projektantom ta uwaga nic nie mówi. Na ich usprawiedliwienie można powiedzieć, że producenci kamer – nie stosując się do zaleceń normy PN-EN IEC 62676-5:2018-09E – skutecznie zatarli różnicę pomiędzy rozdzielczością wizualną kamery a rozdzielczością formatu generowanego przez nią obrazu. Tymczasem „Zasięg DORI" wyliczony na bazie parametrów przetwornika obrazu nie zawiera odniesienia do rzeczywistego zasięgu pola widzenia kamery, w którym operator może realizować dany cel. Co najwyżej umożliwia proste porównanie: kamera A będzie miała większy zasięg niż kamera B. Ale jaki konkretnie użyteczny zasięg będzie miała każda z nich – nie wiadomo. To właśnie kryje się pod sformułowaniem, że podane wielkości zasięgów dają ogólne pojęcie o możliwościach kamery.

Skoro „Zasięg DORI" kamery nie zawiera odniesienia do użytecznego zasięgu jej pola widzenia, to zasadnym pytaniem jest, jak określić ten ostatni. Możliwości są dwie. Pierwsza to obliczenie wykonane na bazie rozdzielczości wizualnej kamery, jeśli jej wartość została wyspecyfikowana przez producenta zgodnie z normą PN-EN IEC 62676-5:2018-09E. Jest to obecnie możliwość czysto teoretyczna, ponieważ producenci kamer powszechnie nie podają tego parametru. Projektantowi chcącemu skorzystać z tej metody pozostaje więc przed obliczeniem zasięgu... wykonanie pomiaru rozdzielczości wizualnej kamer, które zamierza wykorzystać w projekcie. Druga możliwość to pomiar użytecznych zasięgów kamer metodą polowego testu rozdzielczości obrazu, opisaną w normie PN-EN 62676-4:2015-06. Ta metoda została opracowana do stosowania z już zainstalowanymi punktami kamerowymi, ale można ją wykorzystać w testach polowych kamer projektowanych do zastosowania. I choć jest to metoda pracochłonna, daje ona miarodajne wyniki w odniesieniu do użytecznych zasięgów realizacji poszczególnych celów prowadzenia dozoru wizyjnego przez operatora.

Co w tej sytuacji może zrobić projektant pracujący na podstawie typowego zlecenia, czyli takiego, w zakresie którego nie ma pomiarów rozdzielczości kamer bądź testów jakości obrazu? Po pierwsze, musi mieć świadomość tego, co właściwie oznacza podawany w danych katalogowych „Zasięg DORI". Po drugie, musi pamiętać, że narzędzia projektowe do obliczeń zasięgu pól widzenia kamer posługują się parametrami przetwornika obrazu, więc ich obliczenia są tyle samo warte, co „Zasięgi DORI" podawane w kartach katalogowych. Nie pozostaje mu nic innego jak dokonanie ekstrapolacji wyników obliczeń wykonanych za pomocą dostępnych narzędzi projektowych bądź „Zasięgów DORI" podanych w kartach katalogowych i czytelne przedstawienie tego faktu w dokumentach projektu. Ma wówczas naprawdę sporą szansę obronienia swojego projektu, kiedy w sytuacji zaistnienia zdarzenia niepożądanego okaże się, że użyteczne zasięgi pól widzenia są mniejsze niż zasięgi szacowane w projekcie i nie można uzyskać jakości obrazu niezbędnej do realizacji celu prowadzenia dozoru wizyjnego.

Wyjaśnienie, dlaczego zasięg wyliczony na bazie parametrów przetwornika obrazu różni się od zasięgu zmierzonego lub wyliczonego na bazie rozdzielczości wizualnej kamery, jest związane z pojęciami rozdzielczości, opisanymi w normie PN-EN IEC 62676-5:2018-09E.

Rozdzielczość w normie PN-EN IEC 62676-5:2018-09E

Ta część normy określa zalecenia i wymagania dotyczące metod przedstawiania i pomiaru wartości parametrów wydajnościowych, które mają być opisane w materiałach takich jak instrukcje obsługi, broszury i specyfikacje sprzętu kamerowego stosowanego w systemach dozoru wizyjnego. Nie ma więc wątpliwości, że adresatem zaleceń tej normy są przede wszystkim producenci kamer. (Analogicznie do tego, jak adresatami normy PN-EN 62676-4:2015-06 są głównie użytkownicy i projektanci systemów dozoru wizyjnego.)

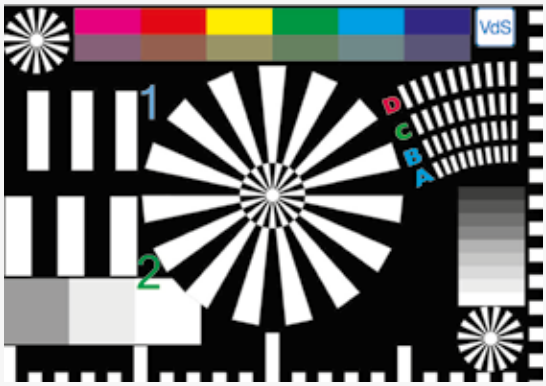
Norma rozróżnia dwa rodzaje rozdzielczości:

- **wizualną,** która jest miarą zdolności kamery (lub systemów wizyjnych) do reprodukcji szczegółów oryginalnej sceny;
- **formatu obrazu** będącą opisem rozmiaru cyfrowego obrazu w pikselach (np. 720P, 1080P, 640 × 480), pikselach na cal lub w liczbie pikseli ramki obrazu.

Tymczasem wielu producentów kamer utożsamia rozdzielczość wizualną kamer z rozdzielczością formatu przetwornika obrazu, ignorując fakt, że liczba pikseli jest niejako „mechanicznym" elementem kamery, a nie jej parametrem wydajnościowym. Liczba pikseli przetwornika obrazu w kamerze wyznacza wyłącznie jej potencjał w zakresie rozdzielczości wizualnej. Nie

jest więc niczym wyjątkowym, że dobra kamera z przetwornikiem o mniejszej liczbie pikseli będzie miała taką samą rozdzielczość wizualną jak kamera z przetwornikiem o większej liczbie pikseli. Różnica pomiędzy rozdzielczością formatu obrazu a rozdzielczością wizualną danej kamery może być w niektórych przypadkach zaskakująco duża, gdyż wpływ na rozdzielczość wizualną kamery mają także zdolność rozdzielcza obiektywu oraz kompresja obrazu w kamerze. Pomiary, które kiedyś wykonaliśmy, pokazały, że kamera 3-megapikselowa (format obrazu 2048x1536 pikseli) miała rozdzielczość wizualną taką jak „idealna" kamera o rozdzielczości formatu 1,3 megapiksela, a kamera 5-megapikselowa (format obrazu 2592x1944 piksele) jak „idealna" 2,8 magapiksela. Tak duża różnica pomiędzy rozdzielczością wizualną a rozdzielczością formatu obrazu jest raczej skrajnym przypadkiem, ale w praktyce może się zdarzyć z wielu różnych powodów.

Wniosek? Użyteczne (rzeczywiste) zasięgi pola widzenia kamery są zawsze mniejsze (czasami sporo mniejsze) niż „Zasięgi DORI" wyliczone na bazie parametrów przetwornika obrazu.



Normatywny obraz testowy do testów jakości obrazu

PN-EN IEC 62676-5:2018-09E – norma napisana dla producentów kamer

Nie spotkałem jeszcze kart katalogowych kamer, w których by napisano, że „Zasięgi DORI" zostały określone na bazie pomierzonej rozdzielczości wizualnej. Ale niby dlaczego producenci kamer mieliby tak określać nienormatywny termin „Zasięg DORI", skoro powszechnie nie specyfikują tak ważnego parametru technicznego kamery, jakim jest rozdzielczość, co zaleca im wprost norma PN-EN IEC 62676-5:2018-09E Systemy dozoru wizyjnego stosowane w zabezpieczeniach -- Część 5: Specyfikacje danych oraz cechy jakości obrazu kamer. Nie specyfikują także pozostałych parametrów technicznych kamery zgodnie z tą normą.

Uwaga zawarta w przywołanej przeze mnie wypowiedzi producenta kamer, że nawet doskonałej jakości i bardzo wysokiej rozdzielczości kamera nie spełni swojego zadania, jeśli przy projektowaniu nie uwzględniono celu prowadzenia dozoru wizyjnego jest w zasadzie skierowana do użytkowników i projektantów. Jest zdecydowanie słuszna, ale miałaby jeszcze silniejszą wymowę, gdyby tenże producent kamer stosował się do zaleceń normy PN-EN IEC 62676-5:2018-09E. Nie udało mi się znaleźć kart katalogowych tego producenta przedstawiających parametry kamer zgodnie z tą normą. Gwoli sprawiedliwości muszę powiedzieć, że nie udało mi się też znaleźć zgodnych z normą danych katalogowych innych producentów kamer. Obecnie (prawdopodobnie) żaden producent kamer przeznaczonych do systemów dozoru wizyjnego nie specyfikuje parametrów zgodnie z w/w normą.

Test jakości obrazu

Ci użytkownicy i projektanci, którzy już na etapie projektu chcieliby znać użyteczne zasięgi pól widzenia punktów kamerowych, muszą najpierw albo zmierzyć rozdzielczość kamer planowanych do zastosowania, albo wykonać testy polowe jakości obrazu, zgodnie procedurą opisaną w normatywnym Załączniku C normy PN-EN 62676-4:2015-06. Ten test wykonuje się zazwyczaj w zainstalowanym systemie, celem sprawdzenia poprawności opracowania i realizacji projektu.

Ktoś może zauważyć, że test wykonany po zakończeniu instalacji systemu dozoru wizyjnego to stanowczo za późno, by dowiedzieć się, jakie użyteczne zasięgi pól widzenia zapewniają zastosowane kamery. Ale dopóki użytkownicy (inwestorzy) i projektanci – np. poprzez izby samorządu gospodarczego – nie skłonią producentów kamer, aby specyfikowali parametry techniczne zgodnie z zaleceniami normy PN-EN IEC 62676-5:2018, dopóty nie będą mieli szans, aby bez uciekania się do pracochłonnych pomiarów i/lub testów poznać rzeczywiste parametry techniczno-użytkowe kamer. Skoro producenci mówią użytkownikom i projektantom systemów dozoru wizyjnego, że powinni postępować zgodnie z normą PN-EN 62676-4:2015-06, to i użytkownicy, i projektanci mogliby powiedzieć producentom, że powinni specyfikować parametry kamer zgodnie z normą PN-EN IEC 62676-5:2018. Zgodność z normą nie dotyczy tylko projektowania i instalacji systemów, ale także urządzeń i oprogramowania.

Czy to koniec „DORI"?

IEC/CENELEC opracował drugą edycję normy EN IEC 62676-4 – projekt końcowy jest obecnie opiniowany przez krajowe organizacje normalizacyjne. Jeśli zostanie zaakceptowany (a wszystko na to wskazuje), to terminy Monitor, Detect, Observe, Recognise, Identify i Inspect przejdą do historii, zaproponowano bowiem nowe terminy: Overview, Outline, Discern, Perceive, Characterise, Validate i Scrutinise. Zamiast dotychczasowego MDORII producenci kamer będą mieli do dyspozycji OODPCVS. Pytanie, co z tym zrobią. Obserwując ich konsekwentne unikanie specyfikowania parametrów technicznych kamer zgodnie z normą i kreowanie własnych marketingowych pseudo-terminów, jestem pewien, że coś wymyślą. •

Waldemar Więckowski
Członek Komitetu Technicznego nr 52 ds. Systemów Alarmowych Włamania i Napadu przy PKN.

Nowe trendy w systemach kontroli dostępu: OD WIEGANDA DO KART WIRTUALNYCH

Przetwarzanie brzegowe oraz algorytmy sztucznej inteligencji spowodowały, że w bezpieczeństwie fizycznym nastąpiła zdecydowana ewolucja. Mobilne systemy kontroli dostępu są jej dowodem.

Jan T. Grusznic

Bazujące na chmurze modele generatywne zyskują na znaczeniu w analizie danych i wspomaganiu decyzji, a urządzenia z wbudowanym przetwarzaniem brzegowym przekształcają sposób, w jaki postrzegamy bezpieczeństwo fizyczne. Trend ten, dominujący dotąd głównie w kamerach dozoru wizyjnego, obecnie dynamicznie rozwija się również w elementach kontroli dostępu.

Nowoczesne urządzenia, takie jak czytniki kontroli dostępu i kontrolery, są wyposażane w jednostki przetwarzania neuronowego, które umożliwiają uwierzytelnianie i analizę danych bezpośrednio na urządzeniu. Dzięki temu eliminowane są opóźnienia wynikające z przesyłania danych do chmury oraz zmniejszane potrzeby infrastrukturalne. W praktyce oznacza to, że takie funkcje, jak liczenie osób, wykrywanie podejrzanych zachowań czy zapobieganie tzw. tailgatingowi (nieautoryzowanemu wejściu za uprawnioną osobą, najczęściej w momencie, gdy drzwi lub bramka są jeszcze otwarte) realizowane są błyskawicznie, bez konieczności angażowania zewnętrznych serwerów.

Sztuczna inteligencja w służbie bezpieczeństwa

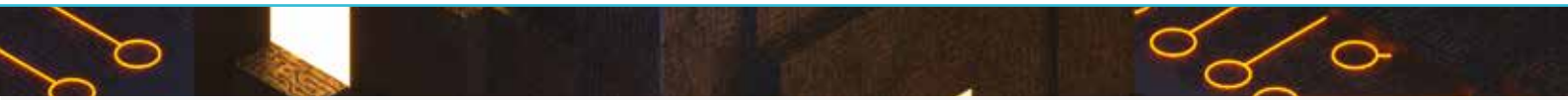
Korzyści płynące z wdrożenia sztucznej inteligencji w systemach kontroli dostępu wykraczają poza szybkie podejmowanie decyzji w czasie rzeczywistym. AI pozwala również na automatyzację wielu procesów, odciąża zespoły bezpieczeństwa i pozwala im koncentrować się na najważniejszych aspektach ochrony środowisk krytycznych. Algorytmy automatyzujące analizę zdarzeń eliminują nadmiar informacji, pozwalając operatorom skupić uwagę na tych incydentach, które rzeczywiście wymagają reakcji.

Jednakże, by sztuczna inteligencja mogła być rzeczywiście uznana za niezawodną, konieczne jest zapewnienie przejrzystości, dokładności i spójności działania. Wyzwaniem pozostaje minimalizacja liczby fałszywych alarmów – wyników zarówno fałszywie dodatnich (odmowa dostępu osobie uprawnionej), jak i fałszywie ujemnych (wpuszczenie osób nieuprawnionych). Szczególnie istotne jest to w podmiotach sklasyfikowanych jako kluczowe wg NIS2, gdzie standardy bezpieczeństwa są wyjątkowo wysokie.

Zarządzanie danymi i zgodność z przepisami

Rozwój systemów biometrycznych, a także coraz szersze wykorzystanie danych osobowych sprawiają, że regulacje prawne odgrywają coraz większą rolę w projektowaniu i eksploatacji systemów kontroli dostępu. RODO oraz niedawno uchwalone rozporządzenie o Sztucznej Inteligencji (AI Act) nakładają na podmioty obowiązek ścisłego przestrzegania zasad dotyczących przechowywania danych, odpowiedzialności oraz uzyskania jednoznacznej, świadomej zgody użytkownika.

W tej rzeczywistości niezwykle pomocne okazuje się zgodność z normami ISO/IEC 27001 (zarządzanie bezpieczeństwem informacji) oraz ISO/IEC 27701 (zarządzanie informacjami o prywatności),



Co to są agenty AI i agentowe systemy AI?

Agent AI to autonomiczny program, który odbiera informacje z otoczenia, podejmuje decyzje i działa na rzecz określonego celu — bez stałego nadzoru człowieka. Może być wirtualny (jak chatbot czy wtyczka automatyzująca zadania) albo fizyczny (jak robot magazynowy). Działa niezależnie, reaguje na zmiany, czasem uczy się na błędach.

Agentowy system AI to cała architektura, zbudowana z wielu takich agentów. Mogą ze sobą współpracować, dzielić zadania i komunikować się, tworząc rozproszony i często złożony ekosystem decyzyjny. To nie tyle pojedynczy byt, ile orkiestra autonomicznych wykonawców, z których każdy gra swoją partię.

Choć pojęcia te bywają używane zamiennie, **agent AI** to jednostka, a **agentowy system** to całość – środowisko, w którym agenci działają razem lub równolegle.

które precyzują zasady postępowania z danymi osobowymi. Jednak ostateczna odpowiedzialność za zgodność z przepisami spoczywa na użytkowniku i administratorze systemu. To oni muszą zadbać o właściwe zarządzanie danymi i wdrożenie procedur zgodnych z obowiązującymi regulacjami.

Agentowa sztuczna inteligencja i autonomiczne procesy

Patrząc w przyszłość, można spodziewać się, że systemy zabezpieczeń będą coraz bardziej autonomiczne. Agentowa sztuczna inteligencja (*Agentic AI*) to nowa generacja systemów, które nie tylko analizują dane i wspierają decyzje. Systemy te są projektowane tak, by mogły samodzielnie podejmować działania i realizować złożone cele. W odróżnieniu od generatywnych modeli AI, których zadaniem jest głównie tworzenie treści, agentowe systemy AI potrafią uczyć się potrzeb zespołów bezpieczeństwa, dostosowywać się do zmieniającego się otoczenia i podejmować proaktywne kroki w celu zapewnienia najwyższego poziomu ochrony – wszystko to przy ograniczonym nadzorze człowieka.

Oczekuje się, że w ciągu najbliższych pięciu lat systemy agentowe zyskają na popularności, przejmując coraz więcej zadań od specjalistów, a tym samym umożliwiając im skupienie się na działaniach wymagających doświadczenia i intuicji.

Ekologia i cyfrowa transformacja

Jednym z najbardziej widocznych trendów w kontroli dostępu jest odejście od fizycznych kart na rzecz rozwiązań cyfrowych. Każdego roku na świecie są sprzedawane setki milionów kart kontroli dostępu, z czego około 20% jest wymienianych z powodu uszkodzeń, zmian technicznych lub rotacji pracowników. Fizyczne karty składają się z różnych materiałów (PVC, PET, biodegradowalne plastiki, chipy, anteny, nadruki), które w praktyce bardzo trudno poddać recyklingowi. Zużyte karty powinny trafiać do odpadów zmieszanych, a nie do żółtych pojemników na tworzywa.

W Polsce rocznie wyrzucana jest ponad tona takich kart. Trafiają one do spalarni lub są przetwarzane mechanicznie. W tej sytuacji rosnącą popularność zyskują rozwiązania mobilne oparte na kartach wirtualnych, które są nie tylko ekologiczną alternatywą, ale oferują również szereg dodatkowych korzyści.

Tymczasem karty wirtualne umożliwiają użytkownikom dostęp do obiektów za pomocą smartfonów lub innych urządzeń mobilnych, eliminując potrzebę korzystania z fizycznych nośników. Rozwiązania te są atrakcyjne nie tylko ze względu na ochronę środowiska, ale także dzięki zaawansowanym mechanizmom bezpieczeństwa, łatwej dystrybucji uprawnień oraz wygodzie użytkowania.

Karty mobilne można wdrożyć jako rozwiązania samodzielne lub zintegrować z istniejącym systemem opartym na fizycznych kartach. Dystrybucja odbywa się automatycznie – użytkownik pobiera kartę i zapisuje ją na swoim urządzeniu. Sposób otwierania przejść można dostosować do potrzeb: od przyłożenia telefonu do czytnika lub potrząśnięcia nim w pobliżu po odblokowanie uprawnień biometrycznie (np. odciskiem palca czy rozpoznaniem twarzy) w newralgicznych strefach. W miejscach, gdzie kluczowa jest wygoda, możliwe jest automatyczne otwieranie przejścia, gdy użytkownik zbliży się do drzwi.

Dla utrzymania kompatybilności z rozwiązaniami mobilnymi kluczowe jest stosowanie czytników obsługujących technologie NFC i/lub BLE. Nowoczesne czytniki wielotechnologiczne pozwalają obsługiwać karty zarówno mobilne, jak i tradycyjne, gwarantując płynne i niedrogie przejście na nową technologię.

Systemy kontroli dostępu przechodzą głęboką transformację, napędzaną przez przetwarzanie brzegowe, sztuczną inteligencję i cyfrową rewolucję kart wirtualnych. Wdrażanie rozwiązań mobilnych nie tylko odpowiada na wyzwania ekologiczne, ale także pozwala organizacjom zwiększyć bezpieczeństwo, elastyczność i wygodę użytkowników. Przed specjalistami ds. bezpieczeństwa stoi wyzwanie: nie tylko nadążyć za tempem zmian, ale także odpowiedzialnie wdrażać nowe technologie, zapewniając zgodność z przepisami i najwyższy poziom ochrony danych. Przyszłość kontroli dostępu jest cyfrowa, ekologiczna i – coraz częściej – autonomiczna. •

Jan T. Grusznic
redaktor „a&s Polska”

Ilustracje: freepik

VISO 2.1.2 – co nowego w systemie kontroli dostępu RACS 5?

Z przyjemnością prezentujemy najnowszą wersję oprogramowania VISO – 2.1.2, która wprowadza szereg istotnych usprawnień, integracji oraz funkcji zwiększających elastyczność zarządzania systemem kontroli dostępu i automatyki budynkowej RACS 5.

Aktualizacja koncentruje się na rozszerzeniu możliwości integracji, poprawie ergonomii pracy oraz rozbudowie funkcji analitycznych i administracyjnych – wszystko to w odpowiedzi na realne potrzeby użytkowników.

Integracje z systemami zewnętrznymi

Jednym z kluczowych obszarów rozwoju jest rozszerzenie integracji z systemami bezpieczeństwa. VISO zyskało możliwość współpracy z systemem ochrony obwodowej **CIAS IB-System IP,** co pozwala na jeszcze skuteczniejsze zabezpieczenie terenu wokół obiektu. Dzięki tej integracji administratorzy mogą reagować na naruszenia stref perymetrycznych w czasie rzeczywistym, bez potrzeby stosowania dodatkowych interfejsów.

Kolejną nowością jest obsługa **kontrolera szafkowego RCC512,** który umożliwia zarządzanie dostępem do szafek depozytowych – rozwiązanie szczególnie przydatne w obiektach sportowych, przemysłowych czy biurowych.

Warto również wspomnieć o integracji z systemem monitoringu wizyjnego **Avigilon Control Center,** która pozwala na synchronizację zdarzeń z systemu kontroli dostępu z materiałem wideo. Dzięki temu operatorzy mogą szybko weryfikować incydenty i podejmować odpowiednie działania.

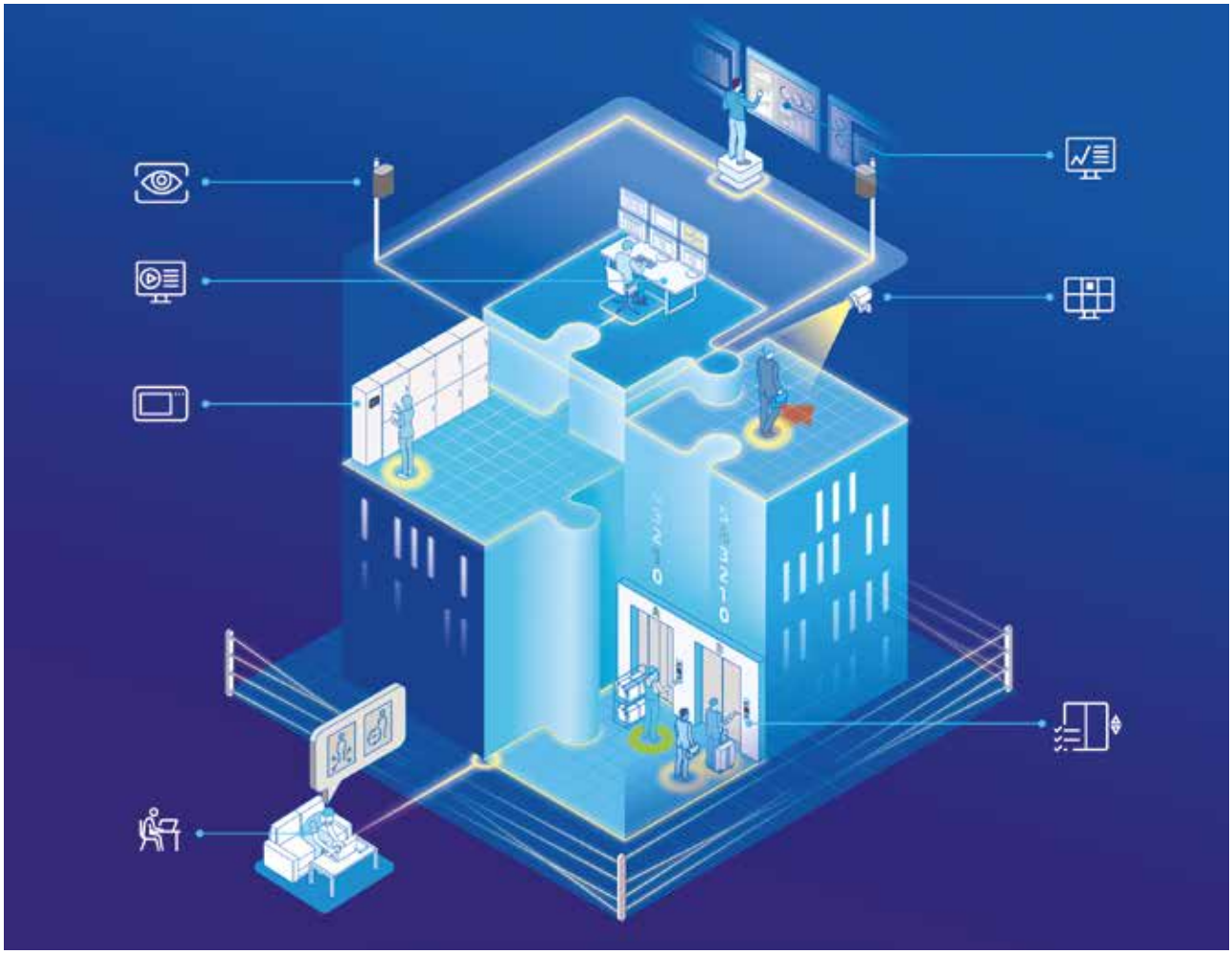
Nowe narzędzia i funkcje użytkowe

Wersja 2.1.2 wprowadza także aplikację **VisitorWEB** umożliwiającą obsługę wizyt przez przeglądarkę internetową. To wygodne rozwiązanie dla recepcji i działów ochrony, które pozwala na zdalną rejestrację gości bez konieczności instalowania dodatkowego oprogramowania.

Z kolei użytkownicy systemów rejestracji i monitorowania obiegu kluczy **RKDS** zyskali możliwość **zdalnego zarządzania kluczami i drzwiami,** co znacząco zwiększa elastyczność i bezpieczeństwo w zarządzaniu dostępem do pomieszczeń i zasobów.

Rozszerzone możliwości analizy i raportowania

Nowa wersja systemu oferuje również **rozszerzone możliwości raportowania i analizy danych.** Administratorzy mogą teraz generować raporty analityczne, które pomagają w ocenie efektywności systemu, identyfikacji nieprawidłowości i planowaniu działań prewencyjnych.



Dodatkowo, możliwy jest **wydruk raportów z notatek na mapach,** co ułatwia dokumentowanie zdarzeń w kontekście przestrzennym.

Usprawnienia systemowe

Wśród licznych usprawnień warto wymienić możliwość przypisywania **harmonogramów aktywności do akcji na zdarzenie,** co pozwala na precyzyjne sterowanie reakcjami systemu w zależności od pory dnia czy dnia tygodnia. Dodano także opcję **dostosowania trybu przejścia do stanu uzbrojenia strefy alarmowej,** co zwiększa elastyczność w konfiguracji zabezpieczeń.

Rozbudowano również funkcje powiadomień SMS – użytkownicy mogą teraz definiować **filtry i harmonogramy,** co pozwala lepiej dopasować komunikację do potrzeb organizacji.

Zarządzanie użytkownikami i wizytami

Integracja z Active Directory została rozszerzona o nowe mechanizmy, takie jak automatyczne przypisywanie użytkowników do predefiniowanych grup czy możliwość ignorowania wybranych grup. Jednocześnie usunięto możliwość importu użytkowników z AD w kreatorze danych, co znacząco porządkuje i upraszcza proces zarządzania kontami.

Moduł Wizyt zyskał funkcję **białej i czarnej listy gości,** co pozwala na automatyczne różnicowanie poziomu dostępu w zależności od statusu osoby odwiedzającej.

Integracje z windami i automatyką

Wersja 2.1.2 rozszerza integrację z systemami windowymi – **Port Technology (Schindler)** o obsługę metody Call by ID, a **KONE Access** o możliwość mapowania typów nośników. To ważne usprawnienia dla obiektów wielokondygnacyjnych, w których kontrola dostępu do wind jest kluczowa.

Dodatkowo rozbudowano również moduł konfigurowania linków do materiałów wideo i zdjęć, dodając możliwość powiązania ich z **węzłami automatyki i centralami pożarowymi,** co zwiększa przejrzystość i szybkość reakcji w sytuacjach alarmowych.

Projektowanie kart

Warto również wspomnieć o usprawnieniach w module projektowania kart – system obsługuje od teraz **nadruk seryjny i dwustronny,** co pozwala na tworzenie bardziej zaawansowanych i estetycznych identyfikatorów.

Podsumowanie

VISO 2.1.2 to wersja, która nie tylko rozwija dotychczasowe funkcje, ale też wprowadza zupełnie nowe możliwości, odpowiadające na potrzeby nowoczesnych systemów bezpieczeństwa. Dzięki integracjom, nowym narzędziom i usprawnieniom platforma staje się jeszcze bardziej elastyczna, skalowalna i przyjazna w codziennym użytkowaniu. •

Roger
Gościszewo 59, 82-400 Sztum
roger@roger.pl
www.roger.pl

BIOMETRIA – oko w oko z deepfake'ami

Jakieś piętnaście lat temu technologie biometryczne kojarzyły się głównie z filmami *science fiction* i futurystycznymi wizjami cyfrowego bezpieczeństwa. Dziś stanowią codzienność, poczynając od ochrony smartfonów po dostęp do stref chronionych w obiektach infrastruktury krytycznej. Biometria stała się synonimem niezawodnego uwierzytelniania, a jej rozwój przyspiesza w niespotykanym tempie. Ta popularność ma jednak swoją cenę.

Monika Żuber-Mamakis

Wiadomo, że każde zabezpieczenie stworzone przez człowieka może zostać przez człowieka pokonane. Popularność biometrii zbiega się w czasie z rozwojem technik wykorzystujących narzędzi SI, szczególności związanych z technikami deepfake i spoofingiem. A coraz łatwiejszy dostęp do narzędzi generatywnej sztucznej inteligencji sprawia, że fałszowanie tożsamości biometrycznej za pomocą deepfake'ów i spoofingu staje się tanie i dostępne nawet dla amatorów. W efekcie najnowszym sposobom biometrycznych zabezpieczeń depczą po piętach równie wyrafinowane techniki służące ich łamaniu.

Jednym z największych zagrożeń dla rozwiązań biometrycznych są techniki bazujące na generatywnej sztucznej inteligencji. Deepfake – choć początkowo traktowany jako narzędzie wykorzystywane do tworzenia wideorozrywki czy propagandy – w kontekście systemów bezpieczeństwa urasta do rangi realnego i rosnącego zagrożenia. Symulacje twarzy, głosu czy ruchu ciała stworzone przez sztuczną inteligencję mogą w wielu przypadkach skutecznie oszukać systemy rozpoznawania biometrycznego, szczególnie te bazujące na danych statycznych i prostych mechanizmach weryfikacji.

Aby w pełni zrozumieć skalę wyzwań, konieczne jest przyjrzenie się bliżej rodzajom biometrii wykorzystywanej w systemach kontroli dostępu. Tradycyjnie dzieli się ją na dwie główne grupy: **biometrię fizyczną** oraz **behawioralną.** Ta pierwsza to rozpoznawanie twarzy, skanowanie odcisków palców, geometria dłoni, analiza tęczówki lub siatkówki oka bądź układu żył dłoni. Druga kategoria obejmuje elementy związane z zachowaniem użytkownika, takie jak sposób mówienia, dynamika pisania na klawiaturze, sposób poruszania się (analiza chodu), a nawet wzorce korzystania z urządzeń mobilnych.

Każde z zabezpieczeń można próbować obejść lub złamać. Dotyczy to także biometrii. Technologia rozpoznawania twarzy, szczególnie popularna w systemach bezdotykowego dostępu i w smartfonach, jest podatna na ataki z wykorzystaniem realistycznych animacji twarzy odtworzonych na ekranie lub generowanych w czasie rzeczywistym awatarów. Przypadki przełamywania zabezpieczeń za pomocą deepfake'owych nagrań twarzy stają się coraz powszechniejsze. Systemy głosowe – stosowane m.in. w bankowości telefonicznej – narażone są z kolei na ataki bazujące na rekonstrukcji głosu użytkownika powstałych na bazie nawet bardzko krótkich próbek dźwięku. Wraz z rozwojem technologii typu *voice cloning* wystarczy zaledwie kilka sekund autentycznego nagrania, by algorytmy opracowały niemal doskonałą kopię głosu, która w wielu przypadkach wystarcza do przejścia procesu uwierzytelniania.

Rozwiązania wykorzystujące odcisk linii papilarnych lub skanowanie oka (tęczówki lub siatkówki) są wprawdzie mniej

podatne na typowe deepfaki, ale przecież nie są w stu procentach odporne na ataki. W ich przypadku wymagają od atakującego po prostu więcej zachodu. Jeśli mowa o odciskach palców, to odnotowano przypadki ich fałszowania za pomocą silikonowych kopii lub precyzyjnych wydruków 3D, które potrafią zmylić starsze lub mniej zaawansowane skanery. W zakresie identyfikacji oka rosnącym problemem są soczewki kontaktowe zawierające nadruk wzoru imitującego rzeczywistą tęczówkę, a także techniki wykorzystujące wysokiej jakości zdjęcia oka pozyskane z mediów społecznościowych lub źródeł publicznych. Dlatego w najnowszych urządzeniach do rozpoznawania tęczówki stosowane są dodatkowe zabezpieczenia przed fałszerstwami. Jednym z takich zabezpieczeń są błyski światła prowokujące źrenicę do kurczenia się. To sprawia, że urządzenie w czasie pomiaru „nie da się" oszukać nadrukiem tęczówki na spreparowanych szkłach kontaktowych.

Biometrii coraz więcej

Wygoda biometrii powoduje, że rośnie skala wdrożeń i inwestycji w te rozwiązania. Już w tym roku światowy rynek biometrii ma osiągnąć wartość ok. 60 mld USD. Jeszcze większą dynamiką wykazuje segment tzw. next-generation biometrics, którego wartość w tym samym roku osiągnie poziom 67,2 mld USD *(Next--Generation Biometrics Market Size, Share & Trends*). Biometria jako usługa (*Biometric-as-a-Service*, BaaS) również notuje szybki wzrost – w 2025 r. wartość tego segmentu rynku sięgnie 3,6 mld USD, niemal trzykrotnie więcej niż pięć lat wcześniej *(Biometric-as-a--Service Market Forecast to 2030)*. W sektorze bankowym, który od lat odgrywa rolę prekursora cyfrowych technologii bezpieczeństwa, aż 87% globalnych banków korzysta z biometrii do uwierzytelniania (Financial Data Consent Trends: Biometric Data and Dynamic Permissions in 2025, stan na marzec 2025). Rynek biometrii w sektorze bankowym wart jest 7,232 mld USD w 2025 r., z prognozą wzrostu do 21,8 mld USD do 2033 r. Bankowość biometryczna będzie rosła ze średniorocznią stopą wzrostu CAGR wynoszącą 14,788% w latach 2025–2033 (dane wg *Biometrics Banking Market Report 2025, Global Edition).*

Popularność ma swoją cenę

Efektem rosnącej popularności biometrii jest to, że staje się celem coraz częstszych ataków. Rosnąca dostępność narzędzi do generowania deepfake'ów oraz demokratyzacja technologii AI sprawiają, że zagrożenia stają się coraz bardziej realne – nawet w przypadku użytkowników indywidualnych czy małych firm.

W 2022 r. ataki typu *digital injection,* kiedy to fałszywe obrazy lub wideo służyły do złamania biometrycznych zabezpieczeń, występowały **pięć razy częściej niż tradycyjne prezentacyjne (np. zdjęcia, maski),** jak wykazał raport biometryczny iProov za rok 2022 *(Biometric Threat Landscape Report Reveals Digital Injection Attacks Now Five Times More Common Than Presentation Attacks)*. Natomiast w drugiej połowie 2023 r. odnotowano spektakularny wzrost ataków typu *face-swap* – aż o **704%** w porównaniu do pierwszej połowy roku (również raport iProov: *New Threat Intelligence Report Exposes the Impact of Generative AI on Remote Identity Verification).* Według prognoz na ten rok ataki typu *digital injection* będą stanowić **ponad 80% wszystkich prób oszustw biometrycznych,** a *face-swap injection* mogą wzrosnąć **trzykrotnie do czterokrotnie** względem poziomów z 2023 wg danych opublikowanych przez VPRanks w artykule *Biometric Hacking: Digital Injection Attacks Take the Lead.*

Rozwiązaniem nie jest jednak rezygnacja z biometrii, lecz jej mądre i warstwowe wdrażanie. Coraz większe znaczenie będą odgrywać systemy multimodalne łączące kilka metod biometrycznych w ramach jednego procesu weryfikacji. Większy nacisk kładzie się też na rozwój sztucznej inteligencji wykrywającej różnego rodzaju odstępstwa od zaprogramowanej normy – nie tylko w samym obrazie czy dźwięku, ale także w zachowaniu użytkownika i metadanych nagrania.

Ważne będą również standaryzacja i regulacje – zarówno po stronie twórców oprogramowania, jak i odbiorców końcowych,

Deepfake – fałszywe, ale bardzo realistyczne, obrazy, filmy lub nagrania uzyskane dzięki narzędziom wykorzystującym SI, a w szczególności sieci neuronowe typu *deep learning* (często GAN – *generative adversarial networks*). *Deepfake* umożliwia np. podmianę twarzy w filmie, wygenerowanie fałszywego nagrania głosu konkretnej osoby lub symulację jej mimiki i ruchu w czasie rzeczywistym. Bywa wykorzystywana zarówno w rozrywce, jak i w działaniach dezinformacyjnych oraz przestępczych, w tym do omijania zabezpieczeń biometrycznych.

Spoofing (w kontekście biometrii) – to technika podszywania się pod inną osobę lub system w celu oszukania mechanizmu uwierzytelniania. W przypadku biometrii może to oznaczać np. wykorzystanie zdjęcia, filmu, nagrania głosu, silikonowego odcisku palca lub sztucznej gałki ocznej imitującej cechy biometryczne prawdziwego użytkownika. Celem *spoofingu* jest przejście przez system zabezpieczeń bez posiadania autentycznych danych biometrycznych.

w tym instytucji publicznych i sektorów infrastruktury krytycznej.

Jednak szczególnie niepokojący jest fakt, że systemy, które były projektowane z myślą o eliminacji haseł i PIN-ów, mogą w niektórych przypadkach stać się łatwiejsze do złamania niż tradycyjne metody uwierzytelniania – zwłaszcza, jeśli nie zawierają mechanizmów potwierdzających, że o dostęp stara się faktycznie człowiek, ale co ważniejsze żywy człowiek. Mowa o tzw. *liveness detection,* czyli detekcji żywotności. To zaawansowana technologia biometryczna, która weryfikuje autentyczność danych pochodzących od żywej osoby. Jej głównym zadaniem jest odróżnienie prawdziwych cech biometrycznych od sztucznych lub zreprodukowanych źródeł, takich jak fotografie, nagrania wideo, maski silikonowe czy syntezowane odciski palców. Jest to pierwsza linia obrony przeciwko **atakom spoofingowym,** w których cyberprzestępcy próbują oszukać systemy biometryczne za pomocą fotografii, nagranych próbek głosu, sztucznych odcisków palców czy masek imitujących ludzką twarz.

W przypadku **systemów rozpoznawania twarzy** analizowane są dynamiczne cechy żywej osoby, takie jak naturalne mrugnięcia, ruchy gałek ocznych, zmiany mimiki oraz głębia obrazu. Dodatkowo można sprawdzać reakcję na polecenia, choćby spojrzenia w konkretną stronę czy wykonanie określonego gestu.

Weryfikacja głosu koncentruje się na unikalnych właściwościach żywej mowy, analizując naturalne intonacje, modulacje głosu oraz wykrywając mikrodrgania charakterystyczne dla ludzkiej krtani. System może również zadawać losowe pytania wymagające odpowiedzi w czasie rzeczywistym, co uniemożliwia użycie wcześniej nagranych próbek.

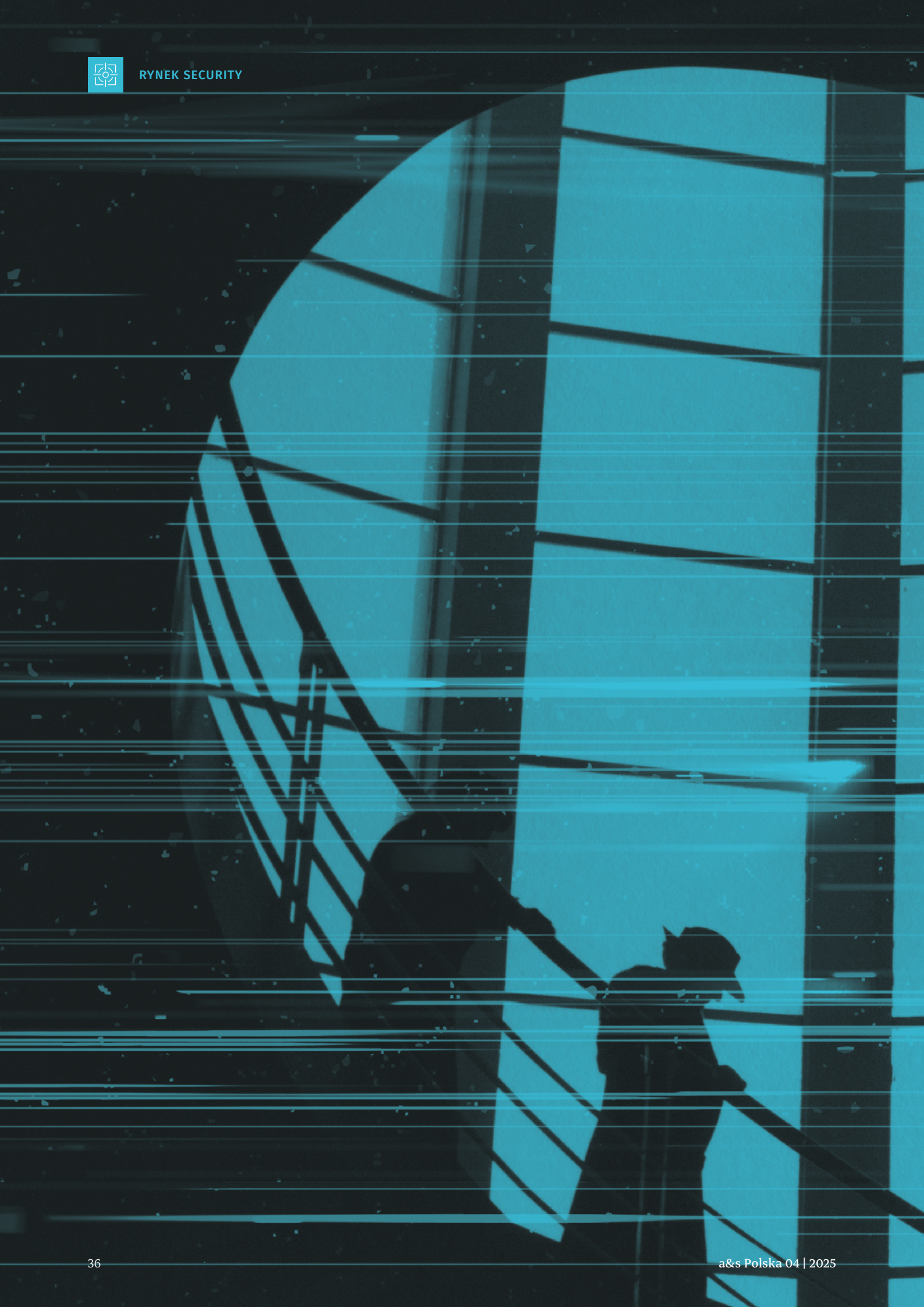
Podczas **skanowania odcisków palców** system bada fizjologiczne właściwości żywej skóry, sprawdzając przewodnictwo elektryczne charakterystyczne dla żywych tkanek oraz subtelne ruchy wynikające z naturalnego drżenia ciała oraz temperaturę i wilgotność powierzchni skóry.

Detekcja żywotności może być pasywna lub aktywna. Pasywna działa w tle, analizując dane bez angażowania użytkownika. System automatycznie bada cechy wskazujące na autentyczność, takie jak naturalna struktura twarzy czy charakterystyczne właściwości głosu. Aktywna detekcja żywotności wymaga zaangażowania osoby sprawdzanej: wykonanie określonych gestów lub ruchów, odpowiedzi na polecenia głosowe lub reakcję na bodźce wizualne lub dźwiękowe.

Biometria w 2025 r. znajduje się w punkcie przełomowym. Z jednej strony stanowi fundament nowoczesnych systemów zabezpieczeń, z drugiej wymaga głębokiej refleksji i dostosowania do realiów nowej epoki cyfrowych fałszerstw. Jej przyszłość nie zależy wyłącznie od postępu technologicznego, ale także od naszej zdolności do rozpoznawania i przeciwdziałania coraz bardziej wyrafinowanym zagrożeniom. W epoce, w której każdy obraz i dźwięk można zmanipulować, prawdziwym wyzwaniem staje się nie tyle identyfikacja człowieka, ile potwierdzenie jego autentyczności – tu i teraz. •

Ilustracje: freepik

Monika Żuber-Mamakis
redaktorka „a&s Polska”



Schron po polsku

Schron, bunkier przydomowy, tymczasowe schronienie – niewielki metraż ma zapewnić bezpieczeństwo w przydomowym ogródku i ochronić najbliższych przed atakiem zbrojnym, opadem radioaktywnym bądź skutkami klęski żywiołowej. Producenci obiecują względny komfort, w którym można przetrwać nawet do miesiąca. Sprawdzamy, jak wygląda rynek schronów w Polsce.

Adela Prochyra

Rynek prywatnych producentów schronów rośnie. Tytułem wstępu należy jednak zaznaczyć, że państwo także ma swój udział w zapewnieniu obywatelom dostępu do schronów i miejsc schronienia. Rok temu w obszernym raporcie „Jak jesteśmy chronieni" pisaliśmy o stanie (nie)gotowości polskiej ochrony cywilnej do radzenia sobie ze skutkami ataków zbrojnych i klęsk żywiołowych. Od tego czasu sytuacja polepszyła się odrobinę – głównie w zakresie ustawodawczym. Chronologicznie rzecz ujmując:

- 10 czerwca 2024 r. Rada Ministrów podjęła uchwałę w sprawie programu „Narodowego Programu Odstraszania i Obrony – Tarcza Wschód". Program zakłada m.in. intensyfikację budowy schronów w Polsce, do czego miał się istotnie przyczynić zakup systemu Ultimate Building Machine (UBM) od amerykańskiej firmy M.I.C. Industries.
- 1 stycznia 2025 r. weszła w życie ustawa z 5 grudnia 2024 r. o ochronie ludności i obronie cywilnej, która m.in. nakłada na inwestorów obowiązek projektowania nowych budynków tak, aby zapewnić w nich możliwość organizacji miejsc doraźnego schronienia. Organy administracji publicznej zobowiązuje natomiast do zaplanowania odpowiedniej ilości miejsc schronienia zbiorowego.
- 27 maja 2025 r. Rząd przyjął Program Ochrony Ludności i Obrony Cywilnej na lata 2025-2026 z budżetami odpowiednio: 16,7 i 17,2 mld zł. Program obejmuje sześć głównych obszarów tematycznych, które mają wzmocnić system ochrony ludności i obrony cywilnej w Polsce. Pierwszy z nich to zapewnienie obiektów zbiorowej ochrony, czyli budowli ochronnych, miejsc doraźnego schronienia oraz centralnej ewidencji takich obiektów.
- 10 czerwca 2025 r. Rada Ministrów przyjęła dawno zapowiadany projekt ustawy o zmianie ustawy – Prawo budowlane oraz niektórych innych ustaw (projekt deregulacyjny). Ułatwia ona m.in. budowę „wolno stojących przydomowych budowli ochronnych, o powierzchni użytkowej do 35 m² (bez zmiany zewnętrznych ścian i konstrukcji)". Budowa będzie odtąd możliwa jedynie na podstawie zgłoszenia, bez konieczności ubiegania się o pozwolenie.

Szeroko komentowana jeszcze rok temu aplikacja Państwowej Straży Pożarnej „SCHRONY" nie została zaktualizowana i dziś ma wartość historyczną – „prezentuje dane, które zostały zebrane na przełomie 2022 i 2023 r. w trakcie ogólnopolskiej inwentaryzacji obiektów budowlanych, w tym budowli ochronnych". Jednocześnie w praktyce niemal nic się nie zmieniło – liczba budowli ochronnych w Polsce nadal – tak samo jak rok, dwa i trzy lata temu – wynosi ok. 62 tys., co oznacza, że wystarczy w nich miejsca dla ok. 1,3 mln ludzi.

Polacy do schronu!

W tym kontekście zupełnie nie dziwi run Polaków na zakup schronów prywatnych. Od wybuchu wojny w Ukrainie zainteresowanie takimi rozwiązaniami ochrony osobistej rośnie lawinowo. Ile dokładnie sztuk sprzedaje się w naszym kraju? Ze względu na niszowy charakter branży liczby nie są podawane do wiadomości publicznej. Wiadomo jedynie, że w Polsce działa od kilku do kilkunastu firm świadczących usługi z tego zakresu – ich liczbę podajemy szacunkowo, ponieważ na ten temat także nie ma oficjalnych statystyk, a GUS ujmuje przedsiębiorców budowlanych zbiorczo. Bywa też, że produkcja schronów to jeden z działów firmy budowlanej. Co więc można ustalić z dużym prawdopodobieństwem? Ceny. Te zaczynają się już od ok. 100 tys. zł za najbardziej proste modele. Najtańszy przydomowy schron 2-osobowy (kategoria ukrycie) można kupić za 120 tys. zł. Podstawowy model 35-metrowego schronu w standardzie deweloperskim z sypialnią i kuchnią kosztuje min. 350 tys. zł netto. Ostateczna cena zależy oczywiście od szczegółów zamówienia, czyli

- Klasy odporności konstrukcyjnej schronu:
  - Kategoria P, czyli podstawowa, chroni przed nadciśnieniem fali uderzeniowej ≥ 0,03 MPa, promieniowaniem jonizującym, odłamkami, pożarami i skażeniami oraz wstrząsami wtórnymi i obciążeniami dynamicznymi;
  - Kategoria A, czyli o zwiększonej odporności i wyższych parametrach wytrzymałości, stosowana jest zwykle w obiektach o znaczeniu strategicznym;
- Wielkości – im większa, tym drożej;
- Materiału konstrukcyjnego: beton prefabrykowany i żelbeton są droższe niż uproszczone metalowe moduły;
- Wyposażenia: specjalistyczne elementy mogą bardzo wpłynąć na cenę, np. same drzwi schronowe w zależności od przeznaczenia (gazoszczelne, przeciwwybuchowe, przeciwodłamkowe itp.) kosztują od ok. 20 do 40 tys. zł. Urządzenia filtrowentylacyjne – kolejne kilkadziesiąt tys. zł.

Najbardziej zaawansowane modele o wysokim standardzie wykończenia i bogatym zaopatrzeniu to koszt przekraczający nawet milion złotych.

Typy schronów

Na rynku komercyjnym dostępne są różne typy schronów przydomowych, wykonane i wykończone w zależności od potrzeb klienta. Te mogą obejmować przypadki takie jak: ochrona przed atakiem zbrojnym, katastrofą naturalną, atakiem chemicznym, ale także ochrona osobista. Rynek odpowiada na najróżniejsze potrzeby, ale zasadniczy podział budowli ochronnych sprowadza się do trzech podstawowych typów:

1. **Schrony naziemne (nadziemne)** umieszczane na powierzchni ziemi, najczęściej przy domu, w garażu lub w ogrodzie. Umożliwiają szybką ewakuację, są łatwe w montażu i w wersji mobilnej można je przenieść w inne miejsce. Typowe przykłady to: bunkry, kontenery pancerne, mobilne schrony z kompozytów, schrony rurowe czy wzmocnione kapsuły.
2. **Schrony podziemne (wkopane w ziemię)** – zakopywane w ogrodzie lub pod domem, najczęściej metodą wykopową, rzadziej górniczą. Są trudniejsze do wykrycia i zapewniają lepszą ochronę przed czynnikami rażenia. Mogą to być modele prefabrykowane – gotowe moduły z betonu/stali montowane w wykopie, zintegrowane z bryłą budynku – ukryte wewnątrz budynku, a także schrony rurowe – wykonane z dużych rur stalowych lub betonowych.
3. **Schrony hybrydowe (naziemno-podziemne),** czyli częściowo zagłębione w ziemi, często z betonowym stropem i ziemią na wierzchu. Stanowią lepszą ochronę niż schrony naziemne i nie wymagają głębokiego wykopu.

Podtypem wszystkich powyżej wymienionych są schrony specjalistyczne, np. NBC – nuklearne, biologiczne, chemiczne – z systemami filtracji powietrza, nadciśnieniem i zapasami żywności. Zapewniają ochronę przed atakiem nuklearnym, chemicznym lub biologicznym, czyli najwyższy poziom ochrony cywilnej.

Jeszcze innym rodzajem zabezpieczenia, również oferowanym przez producentów schronów, jest tzw. *safety room* bądź *panic room,* czyli pokój bezpieczeństwa. Jest to wydzielone, wzmocnione pomieszczenie w istniejącym budynku, które chroni przed napadem, włamaniem, a we wzmocnionej wersji także przed wybuchem.

> Rosnące zainteresowanie klientów, dynamiczny rozwój rynku prywatnych producentów i zmiany w prawie, które upraszczają budowę schronów, wskazują na to, że takie obiekty mogą wkrótce stać się nie ekstrawagancją, lecz elementem standardowego wyposażenia nowoczesnego domu.

Schron jako nowy standard bezpieczeństwa?

Choć jeszcze do niedawna schrony przydomowe uchodziły za fanaberię lub domenę pasjonatów survivalu, dziś coraz częściej postrzegane są jako realne rozwiązanie wobec niestabilnej sytuacji geopolitycznej i/lub coraz częściej występujących gwałtownych zjawisk pogodowych. Rosnące zainteresowanie klientów, dynamiczny rozwój rynku prywatnych producentów i zmiany w prawie, które upraszczają budowę takich obiektów, wskazują na to, że schrony mogą wkrótce stać się nie ekstrawagancją, lecz elementem standardowego wyposażenia nowoczesnego domu. W dobie zagrożeń hybrydowych, ataków cybernetycznych i niepewności militarnej własny schron to nie tylko wyraz przezorności, a być może zupełnie realna inwestycja w bezpieczeństwo bliskich. •

Adela Prochyra
redaktorka „a&s Polska”

Ilustracje: rawpixel

Milestone Technology Day Poland 2025 Inteligentne rozwiązania w różnych branżach

Milestone Systems zaprasza na Milestone Technology Day Poland 2025, który odbędzie się 30 października 2025 roku w Warszawie. Podczas wydarzenia pokażemy, w jaki sposób Milestone wraz z partnerami przekształca różne branże dzięki technologii wideo, inteligentnym integracjom, sztucznej inteligencji, innowacjom w chmurze oraz praktycznym zastosowaniom wykraczającym poza bezpieczeństwo.

Program konferencji obejmie prezentacje liderów branży, sesje poświęcone najnowszym trendom w monitoringu wizyjnym oraz strefę wystawienniczą z udziałem kluczowych partnerów technologicznych, prezentującą na żywo zintegrowane rozwiązania z Milestone XProtect. Uczestnicy zapoznają się ze studium przypadków z handlu detalicznego, miast, sektora energetycznego, transportu i innych. Ilustruje to elastyczność platformy i jej zastosowanie w warunkach rygorystycznych wymagań regulacyjnych.

Podczas Milestone Technology Day Poland 2025 uczestnicy dowiedzą się, jak otwarta architektura XProtect® pozwala na stopniowe rozbudowywanie istniejącej infrastruktury poprzez łączenie rozwiązań PSIM i zabezpieczeń fizycznych z zaawansowanymi funkcjami analityki wideo. Poruszone zostaną tematy szyfrowania strumieni, podpisów cyfrowych oraz mechanizmów kontroli dostępu, które gwarantują integralność danych od momentu rejestracji obrazu aż po ewentualne wykorzystanie materiału dowodowego w sądzie.

Wydarzenie jest skierowane do partnerów, dystrybutorów, architektów systemów (A&E) oraz przedstawicieli sektorów prywatnego i publicznego poszukujących kompleksowych rozwiązań z zakresu bezpieczeństwa fizycznego i cyberbezpieczeństwa.

Milestone ogłosił niedawno projekt Hafnia – inicjatywę w oparciu o AI, która po udanym pilotażu w Stanach Zjednoczonych została uruchomiona w Genui we Włoszech. Projekt ma na celu rozwój zaawansowanych rozwiązań do zarządzania ruchem miejskim oraz budowy inteligentnych miast opartych na wysokiej jakości zbiorach danych wideo w pełni zgodnych z unijnymi regulacjami (RODO, AI Act). Projekt Hafnia wykorzystuje NVIDIA DGX Cloud i narzędzie Nemo Curator do przygotowania rzeczywistych nagrań oraz platformę NVIDIA Cosmos do generowania danych syntetycznych, co umożliwia szkolenie i testowanie wizualno-językowych modeli (VLM) w warunkach odpowiadających realnym scenariuszom miejskim.

Architektura rozwiązania łączy rzeczywiste i syntetyczne nagrania, dzięki czemu VLM uczą się kojarzenia treści tekstowych z obrazami i filmami, co umożliwia generowanie automatycznych podsumowań i analiz wizyjnych. Europejski dostawca chmurowy Nebius zapewnia dedykowaną infrastrukturę GPU, gwarantując pełną suwerenność danych w granicach UE oraz wysoką wydajność obliczeń niezbędną dla aplikacji AI. Projekt dostarcza pierwszy na świecie, w pełni zgodny z unijnymi standardami, otwarty zbiór danych wideo oraz gotowy do wdrożenia model VLM do zarządzania ruchem i transportem miejskim.

Thomas Jensen, CEO Milestone Systems, podkreśla, że Projekt Hafnia stanowi przełom w etycznym rozwoju AI: *Dzięki współpracy z NVIDIA i wsparciu chmury Nebius dostarczamy platformę spełniającą najwyższe wymogi regulacyjne UE, umożliwiając bezpieczne szkolenie i wdrażanie aplikacji AI służących inteligentnym miastom.*

Uczestnicy Milestone Technology Day Poland dowiedzą się, w jaki sposób rozbudowany ekosystem Milestone – obejmujący analitykę AI od BriefCam i chmurowe rozwiązania VSaaS od Arcules – dostarcza kompleksowe rozwiązania i napędza innowacje. Konferencja pokaże studia przypadków, które prezentują płynne integracje tych technologii w różnych środowiskach.

Udział w Milestone Technology Day Poland 2025 jest bezpłatny, liczba miejsc jest ograniczona. Wszystkie prezentacje będą prowadzone w języku angielskim z symultanicznym tłumaczeniem na język polski. To wyjątkowa okazja, aby nawiązać bezpośredni kontakt z zespołem Milestone i partnerami technologicznymi oraz poznać przyszłość monitoringu wizyjnego, łącząc sprawdzone rozwiązania VMS z możliwościami sztucznej inteligencji. •

Zarejestruj się już dziś na oficjalnej stronie wydarzenia **Milestone Systems**

Gdy nie wiadomo o co chodzi, TO WIADOMO, ŻE CHODZI O PIENIĄDZE...

Wszyscy znamy tę maksymę, wszyscy często ją powtarzamy, ale rzadko wnikamy w to, jaki jest całkowity koszt związany z bezpieczeństwem naszych obiektów i operacji. Koncentrujemy się na kosztach głównych, naszym zdaniem najważniejszych, ale czy pomijanie innych kosztów powinno mieć miejsce?

Jacek Grzechowiak

Czy te pomijane koszty są faktycznie niewiele znaczące? Czy ich pomijanie nie powoduje, że zapominamy o inwestycjach ważnych w długim horyzoncie czasowym, których pominięcie lub odłożenie w czasie może przynieść kosztowne konsekwencje?

Pytania tyleż prowokacyjne, co retoryczne. Pytanie zasadnicze, „ile kosztuje ochrona?", jest oczywiście kluczowe, ale dziś chciałbym poszukać innych kosztów ochrony, a raczej braku ochrony.

Ile kosztuje ochrona?

Pytanie „ile kosztuje ochrona?", jest kluczowe, prowadzi nas bowiem do znalezienia kosztów braku ochrony.

Stawka godzinowa – tak to koszt podstawowy w ochronie fizycznej, ale co się za nim kryje? Przecież stawka godzinowa to nie tylko koszt zatrudnienia pracownika, a z tym najczęściej utożsamiamy ten element kosztowy. Stawka godzinowa zawiera kilka ważnych elementów, które mają fundamentalny wpływ na wartość kupowanej usługi ochrony, a więc de facto na nasze bezpieczeństwo. Przyjrzymy się tym elementom.

Szkolenie – najczęściej słyszymy, że agencja ochrony zapewnia „standardowe szkolenia", ale czym one są w praktyce, ile czasu trwają, jaka jest ich częstotliwość, jakie kwalifikacje merytoryczne i dydaktyczne mają osoby je prowadzące? Już tylko te 3 elementy pokazują, że kwota stawki godzinowej może mieć znaczną rozpiętość. Gdy słyszymy, że koszt pracownika waha się w granicach 85-95% ceny usługi, to musi być dla nas jasne, że o szkoleniach w takim przypadku trudno w ogóle mówić. A jeśli już, to będą to szkolenia BHP, wymagane prawem. A gdzie szkolenia z ogólnych zasad ochrony? Gdzie szkolenia profilowe? Gdzie studia przypadków bazujące na obecnej sytuacji geopolitycznej czy obecnej sytuacji w segmencie klienta? Pytania te pozostawiam bez odpowiedzi, licząc na refleksję czytelników.

Umundurowanie – co widzimy najczęściej? Koszulkę z napisem „OCHRONA"? Co agencje ochrony mówią w przypadku umundurowania? Najczęściej: „Do identyfikacji agencji ochrony służy legitymacja pracownika ochrony". Pomijając merytoryczną stronę takiego oświadczenia, warto zdać sobie sprawę, że klient potrzebuje efektywnego narzędzia, pozwalającego odróżnić pracownika ochrony od osoby podszywającej się pod pracownika ochrony. Przykładem jest tu włamanie, do jakiego doszło w jednym z centrów handlowych, gdzie włamywacze pojawili się w ubraniach z napisem „OCHRONA", co pozwoliło im poruszać się po centrum handlowym bez wzbudzania zainteresowania. Incydent miał miejsce już po zamknięciu centrum, kiedy powinny być w nim tylko służby techniczne i ochrona. Jeśli jednak pracownicy techniczni mijają osobę w stroju z napisem „OCHRONA", to skąd mają wiedzieć, że to nie jest przebieraniec? Z legitymacji?! I tu znów dochodzimy do kosztów, bo gdy 85-95% ceny usługi stanowi koszt pracownika, to zapomnijmy o porządnym mundurze, który będzie pierwszym elementem systemu „swój-obcy". Słowo „mundur" ujęte zostało w cudzysłów, bo przecież sama koszulka czy

dowolny inny – z reguły czarny – uniform z napisem „OCHRONA" trudno uznać za mundur.

Wyposażenie – najczęściej widzimy, że pracownicy ochrony posługują się telefonami komórkowymi, niekiedy radiotelefonami – z reguły PMR (*Private Mobile Radio* – rodzaj radiotelefonów, pracujących w paśmie 446,0–446,2 MHz, niewymagających pozwolenia radiowego) – jednak dopatrzenie się zestawów słuchawkowych jest sporym wyzwaniem. Efekt? Opóźniona komunikacja radiowa, a w dodatku słyszalna dla osób postronnych. Co więcej, jeśli w pobliżu mamy budowę, gdzie pracuje jakiś żuraw, którego operator też stosuje te urządzenia, to nadając z wysokości kilkudziesięciu metrów, skutecznie zakłóci pracę urządzeń ochrony. Trudno, by było inaczej, skoro tylko 5, góra 15% pozostaje z ceny usługi po odliczeniu kosztów pracownika ochrony, co nie daje wielkich szans na wyposażenie go w radiotelefon z zestawem słuchawkowym, pracujący w paśmie przeznaczonym dla agencji ochrony. Brak słuchawek nie daje zaś szans na poufność komunikatów. A co jeśli przy pracowniku ochrony stoi napastnik lub terrorysta?

Wyposażenie to także buty. Ileż razy widzieliśmy pracownika ochrony ślizgającego się podczas walki z napastnikiem? Powiem tak, zbyt wiele. Dlatego buty powinniśmy postrzegać nie tylko jako element ubioru. Odpowiednie obuwie to zdecydowanie coś więcej – to narzędzie, które chroni stopy, wspiera postawę i wpływa na ogólne zdrowie. W przypadku pracowników ochrony ma ono szczególne znaczenie. Spędzają przecież długie godziny, stojąc lub robiąc podczas zmiany wiele kilometrów, w zmiennych warunkach i pod presją. W takiej pracy wygodne, odpowiednio dobrane buty to nie luksus, lecz fundament bezpieczeństwa i efektywności pracownika ochrony. Źle dobrane obuwie może prowadzić do bólu stóp, kolan, a nawet problemów z kręgosłupem, czego konsekwencją jest bezpośredni – ale co ważniejsze negatywny – wpływ na refleks, koncentrację i ogólną sprawność, czyli dla pracownika ochrony cechy kluczowe. Lekkość, dobra wentylacja i anatomiczne dopasowanie to cechy, które znacząco zwiększają komfort noszenia – nawet podczas wielogodzinnych zmian. Jak zauważa inżynier ortopedyczny i ekspert ds. ergonomii Lars Eghamn: *Obuwie ochronne musi być wygodne i chronić przed urazami, ale przede wszystkim powinno być zaprojektowane we właściwy sposób*. Tylko wtedy spełnia swoją funkcję – chroni, wspiera i pozwala skupić się na tym, co najważniejsze: skutecznej i bezpiecznej pracy. Czy dobre buty są drogie? Tak ... ale nie myślę tu wcale o cenie buta, lecz innych bardzo realnych kosztach, czyli absencji chorobowej, obniżonej wydajności i ryzyku wypadków. To kolejne koszty, o których dość często zapominamy. To nas prowadzi znów do kosztów. Tam gdzie koszt pracownika ochrony wynosi 85-95% ceny usługi, buty najczęściej kupuje pracownik. A jego wybór może być nieodpowiedni. Klapki, kapcie, buty sportowe ... są na porządku dziennym. Tu o efektywnej ochronie nie mamy co marzyć. A ile razy widzimy pracownika ochrony w rozsznurowanych butach? Przecież to jawny sygnał, że nie jest gotowy do podjęcia swoich obowiązków. Gdy to widzę, od razu wiem, że w jego burach próżno szukać stabilizatora, powodującego łamanie się buta w naturalnym dla naszej stopy miejscu i uniemożliwiającego skręcanie się buta. To brak takiego stabilizatora powoduje zmęczenie nóg, które skutkuje potrzebą dania im odpoczynku poprzez rozsznurowanie. Tak oto podeszwa buta wpływa na bezpieczeństwo. Pamiętajmy też, że but także jest elementem systemu „swój-obcy".

Rękawiczki. Innym ważnym elementem, który często bywa pomijany, są rękawiczki. Rękawiczki w przypadku wielu zadań są niezbędne, zawsze natomiast są przydatne. Pracownik ochrony na placu złomowym, na transporcie kolejowym, patrolujący infrastrukturę w terenie zadrzewionym potrzebuje rękawic. I to nie byle jakich, nie tylko zwiększających poziom ochrony pracownika ochrony i komfort jego pracy, ale także precyzję jego działania, co ma bezpośredni wpływ na skuteczność w sytuacjach wymagających szybkiej reakcji. Wysoka chwytność, trwałość i zręczność manualna, wykończenie typu *touch screen* zapewniające obsługę ekranów dotykowych muszą iść w parze z ochroną dłoni. Dobrze dobrane rękawice to realne wsparcie w codziennej pracy pracownika ochrony – niezależnie od miejsca i rodzaju zagrożeń.

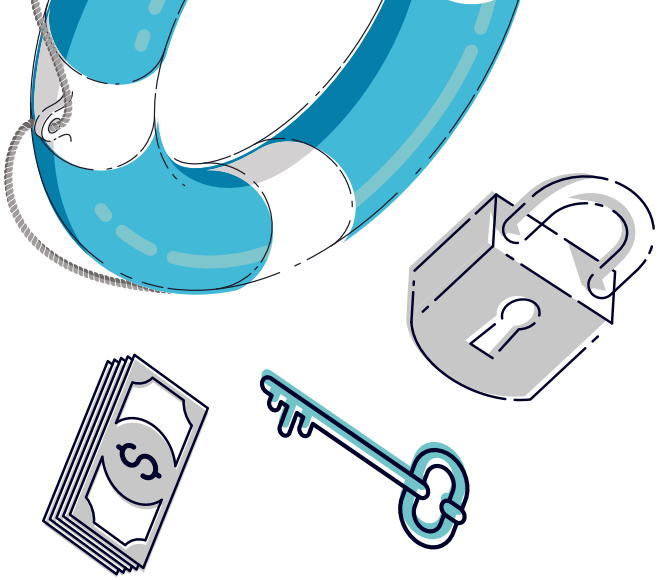
Tych elementów jest oczywiście znacznie więcej, przedstawiam jedynie przykładowe, ale już tylko z tych przykładów widać, że koszty wyposażenia mają swoje odzwierciedlenie w innych pozycjach budżetowych. I tam gdzie agencja ochrony dobrze zainwestuje w wyposażenie, zmniejszy koszty absencji chorobowych, a nawet roszczeń z tytułu niewykonania umowy. Ma to także pozytywne konsekwencje w budżecie klienta, bo przecież kluczowy jest brak incydentów. I mimo że na pierwszy rzut oka zapłaci więcej za ochronę, to zaoszczędzi na innych kosztach, które z reguły są dużo wyższe.

Jak to wygląda z perspektywy klienta?

Omówione powyżej elementy mogą być mocnym bądź słabym punktem ochrony. A jak widać ich sklasyfikowanie jest banalnie proste.

Trzeba jednak wiedzieć, że koszt ochrony to nie tylko koszt umowy z agencją ochrony. Elementów składowych jest trochę więcej. Zaczynają się od kosztu odtworzenia mienia ukradzionego lub zniszczonego w wyniku braku ochrony. Jego wysokość bywa różna i zależy nie tylko od wartości odtworzeniowej mienia. Ważnym czynnikiem jest dostępność mienia. Czasami nie można

„...koszt ochrony to nie tylko koszt umowy z agencją ochrony. Elementów składowych jest trochę więcej. Zaczynają się od kosztu odtworzenia mienia ukradzionego lub zniszczonego w wyniku braku ochrony.



odkupić raz skradzionych rzeczy (nawet zamienników), bo np. nie są już produkowane, albo ich produkcja jest możliwa tylko na zamówienie. Koszt odtworzenia może więc zawierać także koszt przeprojektowania systemów lub wynajęcia i eksploatacji rozwiązań zastępczych. W skrajnym przypadku mogą dojść koszty przestoju.

Należy doliczyć także koszt zarządzania kryzysowego, z którym jest związany każdy incydent. Kradzież, włamanie czy dewastacja zawsze wymagają pilnego działania określonej grupy pracowników, a tym samym oderwania ich od ich zasadniczych zajęć. Należy o tym pamiętać, by wiedzieć, jak będzie w takiej sytuacji funkcjonować biznes. Natomiast po powrocie do stanu normalnego pojawia się potrzeba przeanalizowania incydentu w celu wyciągnięcia wniosków na przyszłość. I tu przecież także mamy konkretne koszty, które możemy i powinniśmy oszacować. I nie jest to skomplikowane, bo przecież każdy z nas dostaje miesięczną wypłatę, a więc nasza stawka godzinowa jest znana. Podsumowanie godzin poświęconych na analizę incydentu da konkretny koszt. Proporcje tych kosztów na poziomie klienta i na poziomie agencji ochrony wyglądają odmiennie, wynika to z profilu tych organizacji. Klient będzie to porównywał do wartości niewyprodukowanych wyrobów lub niezrealizowanych usług, powiększonych o kary umowne. Natomiast agencja ochrony będzie to porównywała do wartości swoich usług w danym kontrakcie. Przy czym należy tu patrzeć nie na wartość kontraktu, tylko na jego marżę. W znanych mi przypadkach zdarzało się, że koszt analizy incydentu przewyższał wartość straty. I to zarówno w agencjach ochrony, jak i u klientów.

Pośrednie koszty incydentów również mają znaczenie

Kolejnym kosztem braku ochrony to koszt utraty wizerunku. Uważa się go za niewymierny, ale warto jest podjąć się próby jego oszacowania. Dobrym przykładem są tutaj galerie handlowe, które doskonale wiedzą, jak spada frekwencja po każdym – nawet fałszywym – alarmie bombowym. Mniej odwiedzających to niższa sprzedaż, ergo koszt utraty wizerunku wynikający z incydentu, przekłada się na klasyczną stratę finansową. W firmach produkcyjnych i usługowych to także można policzyć. W agencjach ochrony – które przecież są typowymi firmami usługowymi – także można to zrobić. Jeśli klient polecał nas wcześniej, a teraz przestał polecać, to połączenie tego z incydentem wydaje się oczywiste. A koszty można wyliczyć z wartości umów zawartych na podstawie wcześniejszych poleceń. Utrata wizerunku to także negatywne oddziaływanie na przyszłe kontrakty. Tu wyliczenie jest oczywiście trudniejsze, ale potencjalny klient nie będzie ryzykował współpracy z firmą, w której może dojść do incydentu, co może przecież przełożyć się na niemożność wykonania umowy, niedostarczenie produktów lub usług w wymaganym czasie, ilości i jakości, a więc do pojawienia się poważnych problemów z jego operacjami. Może dojść do sytuacji, w której kary umowne wynikające z zaistniałego incydentu mogą być najmniejszym problemem, bo klient po prostu nie powierzy nam kolejnych projektów. W skrajnym przypadku utrata reputacji może zaprowadzić do konieczności zakończenia działalności gospodarczej. Historyczne przykłady, takie jak incydent w Hatton Garden, są tu bardzo wymowne.

Brak ochrony to także koszty prawne związane z postępowaniami sądowym, współpracą z organami ścigania – kolejne godziny naszych pracowników, koszty nośników, które musimy zabezpieczać, niekiedy koszty związane z montażem zamiennych zamków w miejsce tych, które zostały przekazane do badań mechanoskopijnych, czy koszty zakupy macierzy CCTV. Kategorie są właściwie ograniczone jedynie wyobraźnią sprawców, którzy mają niezliczone metody działań. A wszystko to powiększone o koszt obsługi prawnej niezbędnej, by sprawcę postawić przed obliczem wymiaru sprawiedliwości i ewentualnie – z dużym naciskiem na to słowo – skazać go i zabezpieczyć jego mienie celem pokrycia naszych strat.

Kolejnym kosztem jest spadek produktywności. Jest to element najtrudniejszy do oszacowania, ale występuje zawsze. Każdy incydent powoduje rozmowy między pracownikami, którzy w naturalny sposób reagują na nadzwyczajną sytuację, jaką jest kradzież czy włamanie. To oznacza, że pracują mniej efektywnie. Można to oszacować, porównując produkcję przed incydentem i po incydencie. W usługach jest nieco trudniej, ale także można wycenić wydajność pacy, porównując czasy wykonania poszczególnych usług sprzed incydentu i po nim. To trudne zadanie i niestety mające oczywiście swoją cenę.

Koszty pracownicze także potrafią ucierpieć – w niektórych kategoriach incydentów pojawiają się obawy pracowników o ich bezpieczeństwo w miejscu pracy, co prowadzi nie tylko do spadku produktywności, ale także konieczności inwestycji w różnego rodzaju programy mające na celu zniwelowanie tych obaw. Liczyć się należy także z odejściami pracowników, które skutkują nie tylko koniecznością zatrudnienia nowych, a więc kosztami rekrutacji i wdrożenia, ale także wielomiesięcznym ryzykiem kolejnych odejść, powodując, że problem związany z pracownikami może potrwać naprawdę długo.

Jak więc widzimy, prawdziwe koszty braku ochrony mogą być poważnym problemem. A czy będą? To już zależy od nas. •

Jacek Grzechowiak
Menedżer ryzyka i bezpieczeństwa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych. W przeszłości związany z grupami Securitas, Avon i Celsa, w których zarządzał bezpieczeństwem i ryzykiem. Właściciel firmy RISKRESPONSE. Dyrektor Centrum Kompetencji „a&s Polska".

Ilustracje: freepik

TELEDYNE FLIR

Elara™ Seria R

System radarowy z bardzo szerokim poziomym polem widzenia 90°, umożliwiający monitorowanie dużych obszarów

Skuteczne wykrywanie w trudnych warunkach

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

OFICJALNY DYSTRYBUTOR:

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

WWW.LINC.PL

Linc Polska Sp. z o.o.


FLIR
FLIR

Głos branży

Nowoczesne technologie stają się kluczowym wsparciem w pracy facility managera, umożliwiając efektywne zarządzanie budynkami i infrastrukturą. Coraz większą rolę odgrywają automatyzacja procesów oraz integracja systemów budynkowych, w tym nowoczesnych zabezpieczeń elektronicznych, które usprawniają codzienne operacje i wspierają realizację strategii zrównoważonego rozwoju. Wraz z rozwojem takich rozwiązań pojawia się pytanie, czy w obliczu postępu technologicznego warto zrezygnować z usług tradycyjnych agencji ochrony. Sprawdź, jak na to zagadnienie patrzą eksperci branżowi.

Mądry Polak po szkodzie

KRZYSZTOF ŁĘCKI
TAURUS OCHRONA GROUP, PIO

Tym przysłowiem mógłbym spuentować odpowiedź na pytanie czy warto rezygnować z usług firm ochrony. Jednak temat jest bardziej złożony. Wielu przedsiębiorców rozważa ograniczenie kosztów poprzez rezygnację z usług koncesjonowanych agencji ochrony, zastępując je pracownikami wewnętrznymi lub polegając wyłącznie na polisie ubezpieczeniowej. Taka decyzja, choć pozornie racjonalna finansowo, może nieść istotne ryzyko prawne i operacyjne. Odpowiedzi warto szukać w przepisach, standardach branżowych i analizie kosztów.

Niektórzy klienci próbują chronić się samodzielnie, ale to rozwiązanie ma ograniczenia. Taki pracownik może co najwyżej dokonać obywatelskiego ujęcia, lecz nie ma prawa stosować środków przymusu ani legitymować. Nie może też być nazywany „pracownikiem ochrony", bo taki tytuł przysługuje tylko pracownikom zatrudnionym w koncesjonowanej agencji ochrony – to po prostu dozorca. Niekiedy firmy, chcąc uniezależnić się od agencji, tworzą własną Wewnętrzną Służbę Ochrony (WSO), ale uzyskanie takiego zezwolenia bywa trudne, a jej utrzymanie kosztowne z uwagi na ulokowanie kosztów administracyjnych w jednej strukturze firmy.

Ubezpieczenie i usługi ochrony opierają się na różnych przepisach, a ich cel jest odmienny. Ubezpieczenie ma wypłacić odszkodowanie od ryzyk nieprzewidzianych po zaistniałym zdarzeniu. Ochrona ma w swoim założeniu przeciwdziałać zdarzeniom, które z analizy zagrożeń da się przewidzieć, zapewniając staranność przy zastosowaniu odpowiednich środków technicznych i fizycznych. Często zapisy polisy obligują klienta do zabezpieczenia technicznego mienia oraz zapewnienia ochrony przez koncesjonowaną agencję ochrony.

Agencja ochrony, świadcząc usługi ochrony dla wielu klientów, dysponuje wieloma narzędziami, których nie sposób zastąpić przy zapewnianiu bezpieczeństwa własnymi zasobami. Agencje ochrony muszą posiadać koncesję. Czyli dokument, który jest wydawany na podstawie procedury sprawdzającej sam podmiot oraz osoby kierujące danym podmiotem. Poza tym podmiot ten zobligowany jest posiadać polisę ubezpieczeniową. Kwalifikowani Pracownicy Ochrony zatrudnieni przez agencję ochrony z mocy art. 36 ust. 1 UOOIM mają uprawnienia m.in. do legitymowania, ujęcia osoby, użycia środków przymusu czy broni palnej. Agencje ochrony zobligowane są do szkoleń swoich pracowników, a pracownicy przechodzą regularne badania. Wszystko to wymaga tworzenia struktur odpowiedzialnych za te zadania. Przy analizie kosztów warto wziąć pod uwagę nie tylko koszty bezpośrednie zatrudnienia pracownika, ale również nakłady na umundurowanie, wyposażenie, logistykę, koszty nadzoru. Koszty te, w agencji ochrony, rozkładają się na wszystkich klientów, a co za tym idzie koszt jednostkowy przypadający na klienta jest mniejszy.

Jednak chcąc w pełni skorzystać z prerogatyw koncesjonowanej agencji ochrony, należy wziąć pod uwagę profesjonalizację koncesjonowanych podmiotów, na które wpływają nie tylko zapisy ustawowe, ale także elementy wynikające ze standardów jak posiadana wielkość polisy oraz klauzule w niej zawarte, wdrożone systemy zarządzania potwierdzone certyfikatami, np. ISO, elektroniczne systemy nadzoru oraz wykorzystywanie nowoczesnych technologii do realizacji usług ochrony oraz zarządzania, jak również doświadczenie potwierdzone referencjami oraz zasobami finansowymi.

Wniosek? Rezygnacja z profesjonalnej ochrony może być pozorną oszczędnością, prowadzącą do większych kosztów i ryzyka w przypadku incydentu.

Ochrona to nie koszt, to inwestycja

MARCIN PYCLIK
POLSKA IZBA OCHRONY

We współczesnym świecie jest wiele zagrożeń – od rosnącej przestępczości, przez cyberataki, aż po klęski żywiołowe i kryzysy społeczne. W takich realiach bezpieczeństwo staje się nie tylko potrzebą, ale także fundamentem normalnego funkcjonowania społeczeństwa, w tym biznesu. Dlatego rezygnacja z usług firm ochrony – zarówno fizycznej, jak i technicznej – może prowadzić do poważnych konsekwencji.

Pierwszym powodem, dla którego nie warto rezygnować z ochrony, jest prewencja. Obecność ochrony działa odstraszająco na potencjalnych sprawców przestępstw. Widoczna obecność pracownika ochrony fizycznej, skuteczny monitoring wizyjny, patrole prewencyjne grup interwencyjnych z pewnością zmniejszają ryzyko kradzieży, włamań, aktów wandalizmu, a nawet zamachów o charakterze terrorystycznym. Ochrona to nie tylko reakcja na zagrożenie, to przede wszystkim zapobieganie i wzmacnianie odporności obiektu.

Drugim aspektem jest szybka reakcja. W sytuacji kryzysowej każda minuta ma znaczenie. Służby ochrony są przeszkolone, by podejmować decyzje pod presją czasu i działać zgodnie z procedurami. To może uratować życie, zdrowie lub znacznie ograniczyć straty materialne. Bez obecności ochrony reakcja na zagrożenie jest opóźniona, a odpowiedzialność często spada na osoby, które zupełnie nie są przygotowane na taką sytuację.

Nie można też pominąć poczucia bezpieczeństwa. Pracownicy firm, klienci sklepów, mieszkańcy osiedli – wszyscy czują się pewniej, gdy wiedzą, że ktoś czuwa nad ich bezpieczeństwem. To zwiększa komfort życia, efektywność pracy i pozytywnie wpływa na wizerunek miejsca pracy, życia i wypoczynku.

Ochrona to również ochrona ubezpieczeniowa. Każda firma ochrony jest obowiązkowa ubezpieczona od odpowiedzialności cywilnej, od nienależytego wykonania swoich zadań. Ponadto agencje ochrony mają również dodatkowe ubezpieczenie nadwyżkowe na sumy sięgające kilku lub nawet kilkunastu milionów złotych. Jest to ważny element zapewniający materialną ochronę w przypadku wystąpienia strat w mieniu.

Wreszcie ochrona to nie koszt, to inwestycja. Koszty wynikające z włamania, zniszczeń czy przestoju działalności są często znacznie wyższe niż wydatki na ochronę. Zawsze lepiej zapobiegać niż później leczyć.

W obliczu coraz bardziej nieprzewidywalnych zagrożeń rezygnacja z ochrony jest decyzją ryzykowną. Bezpieczeństwo nie powinno być luksusem, lecz stałym elementem codzienności – w życiu zarówno prywatnym, jak i zawodowym.

Adekwatne środki ochrony

KRZYSZTOF BARTUSZEK
SECURITAS POLSKA

Niestabilność polityczna, migracje, rozwarstwienie społeczne, wojny to tylko niektóre makro-zmienne, które kształtując dzisiejszą rzeczywistość, wpływają na poziom zagrożeń w bankach, biurowcach, hotelach czy też innych obiektach.

Statystyki przestępczości pokazują jasno – nie żyjemy w bezpiecznych czasach, a mimo to zachowujemy się, jakby tak było. Jeszcze kilka lat temu o zastosowaniu odpowiednich sił i środków związanych z bezpieczeństwem decydowali fachowcy, dobierający elementy adekwatnie do zagrożeń. W ostatnich latach coraz częściej rolę decydenta przejmuje arkusz kalkulacyjny.

Oczywiście nie wszędzie i nie wszystkich charakteryzuje takie podejście. Bardziej świadome organizacje podchodzą do bezpieczeństwa poważnie i w oparciu o rozbudowane analizy ryzyka zarządzają swoim bezpieczeństwem. Niestety mam poczucie, że takich organizacji z roku na rok jest coraz mniej i nawet nie ich wielkość świadczy o ich dobrych lub złych nawykach. Coraz częściej decyzyjność w zakresie doboru składowych systemów bezpieczeństwa jest przekazywana w ręce osób odpowiedzialnych za zakupy. I nie byłoby w tym nic złego, bo cena jest i będzie ważna.

Problem w tym, że w procesach definiowania zapytań ofertowych coraz mniej jest pytań o ryzyka i adekwatne do nich środki. Coraz częściej zapytania ograniczają się do pytania o cenę za godzinę czy też za sztukę, za urządzenie lub abonament.

W przypadku rozwiązań IT kwestia decyzyjności poszła w zupełnie w inną stronę – tam opinię specjalistów uznajemy za prawdy objawione, stanowiące punkt wyjścia do dalszych działań i decyzji. Dlaczego więc uznaliśmy, że bezpieczeństwo fizyczne nie ma znaczenia? Przecież nawet systemy informatyczne zabezpieczone przed cyberatakiem będą bezsilne, jeśli ktoś fizycznie uszkodzi serwer lub podpali obiekt – czego notabene w ostatnich miesiącach kilkukrotnie byliśmy świadkami.

Otoczenie, w którym działają banki, biurowce, hotele, ale i inne obiekty, stale się zmienia – zmieniają się zagrożenia, a także nawyki i oczekiwania pracowników, klientów oraz gości. Poczucie bezpieczeństwa jest podstawową potrzebą każdego człowieka, tym bardziej niepokojące jest uproszczenie podejmowania decyzji w tym zakresie.

Życzyłbym sobie i wszystkim decydentom, byśmy wrócili do systematycznej oceny ryzyka, która będzie podstawą do określenia adekwatnych środków ochrony.

Cena powinna być ważna, ale niech będzie podsumowaniem wartości nabytych towarów i usług, a nie jedynym kryterium ich wyboru.

Nowoczesna technologia dla facility managera

ARKADIUSZ RYMARSKI
HONEYWELL

Od blisko trzech dekad obserwuję ewolucję podejścia do kwestii bezpieczeństwa w zarządzaniu obiektami. W regionie Europy Środkowo-Wschodniej, gdzie nowoczesne biurowce funkcjonują obok wciąż eksploatowanych budynków z lat 70., jedno pozostaje niezmienne: skuteczna ochrona ludzi, danych oraz infrastruktury nie jest dziś możliwa bez zastosowania zintegrowanych rozwiązań technologicznych.

W wielu obiektach infrastruktura bezpieczeństwa obejmuje systemy pochodzące od różnych dostawców – kamery jednego producenta, kontrola dostępu innego, system alarmowy jeszcze innego. Przez to w sytuacjach kryzysowych często często dochodzi do dezorganizacji oraz opóźnionej reakcji. Dlatego coraz większe znaczenie zyskują zintegrowane platformy, takie jak Honeywell Enterprise Buildings Integrator (EBI), które łączą w jednym środowisku systemy CCTV, kontroli dostępu, sygnalizacji włamania i napadu, systemy pożarowe i energetyczne. Dzięki temu facility manager ma jeden pulpit sterowania – z pełnym obrazem sytuacji i możliwością reagowania w czasie rzeczywistym, także zdalnie.

Jednakże samo połączenie systemów to dziś za mało. Nowoczesne rozwiązania wykorzystują sztuczną inteligencję (AI), która analizuje dane z czujników, identyfikuje nieprawidłowości i uczy się wzorców. Jeśli AI wykryje nietypowy ruch w strefie parkingowej w nocy albo wzrost temperatury w serwerowni – może powiadomić ochronę, uruchomić odpowiednie procedury lub nawet zapobiec awarii. Takie podejście nie tylko zwiększa bezpieczeństwo, ale pozwala też zmniejszyć liczbę fałszywych alarmów, obniżyć koszty i podnieść efektywność operacyjną.

Coraz ważniejszym elementem staje się cyberbezpieczeństwo. W dobie powszechnego podłączania urządzeń do sieci systemy bezpieczeństwa same stają się celem ataków. Wystarczy luka w zabezpieczeniach, by zdalnie wyłączyć alarmy czy odblokować drzwi. Dlatego dziś standardem są mechanizmy szyfrowania, uwierzytelnianie wieloskładnikowe oraz monitoring anomalii, również w rozwiązaniach Honeywell, które traktują bezpieczeństwo cyfrowe jako integralny element infrastruktury.

Bezpieczeństwo to również dbałość o komfort użytkowników. W kontekście pracy hybrydowej oraz zwiększonej świadomości w zakresie zdrowia coraz więcej budynków wykorzystuje czujniki jakości powietrza (IAQ), by kontrolować poziom CO_2, pyłów czy lotnych związków. Systemy wentylacyjne reagują automatycznie, dostosowując parametry do realnych potrzeb, co wpływa na zdrowie, samopoczucie i efektywność pracy. To nie tylko ukłon w stronę ESG *(Environmental, Social, Governance* – środowisko, społeczna odpowiedzialność i ład korporacyjny), ale też realna korzyść biznesowa.

Na bazie mojego doświadczenia mogę stwierdzić, że właściwie wdrożona technologia nie komplikuje procesów zarządzania, wręcz przeciwnie – znacząco je upraszcza i czyni bardziej przewidywalnym. Dostarcza facility managerowi narzędzi umożliwiających podejmowania decyzji w oparciu o rzetelne dane, zamiast intuicyjnych założeń. W realiach, w którym niepewność stała się stałym elementem funkcjonowania, taka przewaga ma kluczowe znaczenie.

Zabezpieczenia hoteli

MARCIN WALCZUK
BCS

Współczesny hotel to nie tylko miejsce wypoczynku, lecz także obiekt wymagający zaawansowanych rozwiązań z zakresu bezpieczeństwa technicznego. Rosnące oczekiwania gości, a także obowiązki prawne skłaniają właścicieli hoteli do wdrażania kompleksowych zabezpieczeń chroniących ludzi, mienie i dane.

BCS w swojej ofercie ma pełną gamę urządzeń, które idealnie sprawdzą się w zabezpieczaniu nawet największych obiektów hotelowych. Podstawą technicznego zabezpieczenia hoteli są systemy kontroli dostępu. Elektroniczne zamki z kartami RFID, kodami PIN czy aplikacjami mobilnymi pozwalają zarządzać ruchem gości i personelu, minimalizując ryzyko nieautoryzowanego wejścia.

Kluczową rolę zarówno prewencyjną, jak i operacyjną odgrywa monitoring wizyjny. Kamery dozorowe rozmieszczone w strategicznych punktach – wejściach, lobby, windach, korytarzach, parkingach czy strefach technicznych – umożliwiają bieżącą kontrolę nad tym, co dzieje się na terenie obiektu. Wysokiej jakości obraz, inteligentna analiza obrazu i integracja z systemami alarmowymi pozwalają szybko reagować na zagrożenia, podejrzane zachowania czy sytuacje awaryjne.

Dla personelu recepcji i służb ochrony monitoring jest nieocenionym narzędziem codziennego nadzoru operacyjnego. Pozwala śledzić przepływ gości, kontrolować obciążenie stref wspólnych, a także dokumentować ewentualne incydenty. W razie konieczności nagrania stanowią ważny materiał dowodowy.

Nowoczesne systemy monitoringu BCS można zintegrować z oprogramowaniem hotelowym, co umożliwia np. automatyczne otwieranie drzwi po rozpoznaniu twarzy gościa bądź śledzenie tras przemieszczania się personelu technicznego w celach optymalizacji pracy.

Istotną kwestią pozostaje zgodność z przepisami dotyczącymi ochrony danych osobowych. Monitoring musi być odpowiednio oznakowany, a nagrania przechowywane zgodnie z regulacjami RODO. Wdrażając system telewizji dozorowej, hotel powinien również opracować politykę dostępu do materiałów wizyjnych oraz procedury w zakresie prywatności gości.

Inwestycja w monitoring to nie tylko poprawa bezpieczeństwa – to także wzrost zaufania klientów i lepsza kontrola procesów wewnętrznych. W czasach wzmożonych oczekiwań co do komfortu i ochrony prywatności telewizja dozorowa stanowi podstawę technicznego zabezpieczenia każdego hotelu.

Niemniej istotne są systemy przeciwpożarowe – detektory dymu, czujniki temperatury i automatyczne tryskacze, połączone z centralą alarmową, umożliwiają szybką reakcję w razie zagrożenia. Dopełnieniem są ewakuacyjne oświetlenie awaryjne oraz czytelne oznaczenia dróg ewakuacyjnych.

Bezpieczeństwo w hotelach zyskuje nową jakość

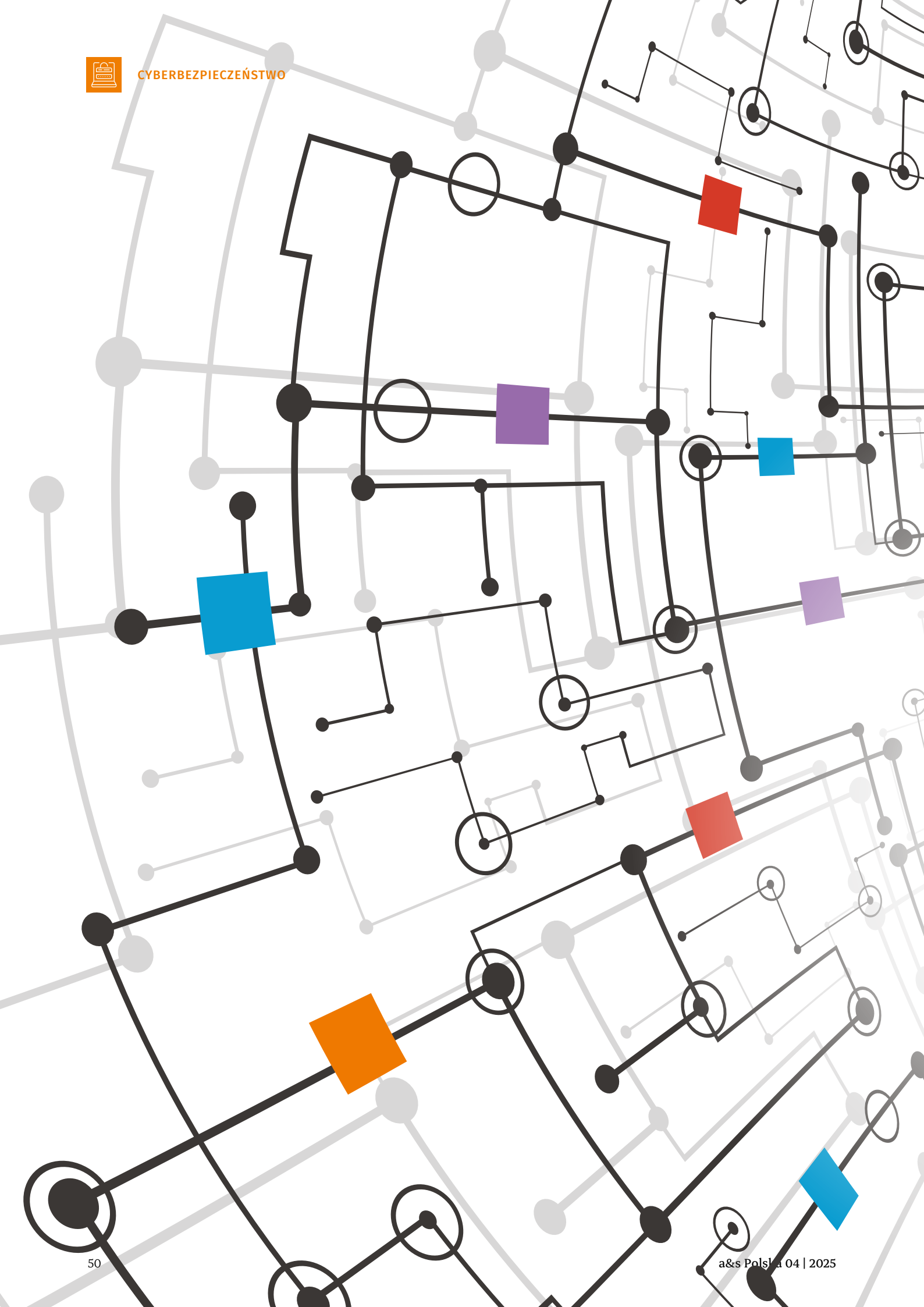
BARBARA PODWYSOCKA
POLSKI HOLDING HOTELOWY

Integracja systemów bezpieczeństwa w hotelach staje się dziś standardem, który nie tylko podnosi poziom ochrony, ale też zwiększa efektywność pracy personelu. Połączenie w spójną całość kontroli dostępu, monitoringu wizyjnego, systemów sygnalizacji pożarowej oraz czujników środowiskowych pozwala na szybkie zbieranie informacji, analizę zdarzeń i natychmiastową reakcję. Kluczowe jest przy tym uwzględnienie zmieniających się czynników zewnętrznych i wewnętrznych – zarówno w otoczeniu obiektu, jak i w samej jego strukturze organizacyjnej.

Goście oczekują nie tylko bezpieczeństwa fizycznego, ale także dyskrecji, ochrony swoich danych i wizerunku. Zmienia się również profil pracownika – nowe pokolenia cenią sobie narzędzia, które ułatwiają im pracę i pozwalają skupić się na obsłudze gości. Dlatego projektując systemy zabezpieczeń, warto brać pod uwagę te aspekty i łączyć je z możliwościami, jakie daje technologia.

Niezmiennie najważniejszym elementem systemu bezpieczeństwa w hotelarstwie pozostaje człowiek – to pracownik jest tym, który podejmuje decyzje i reaguje w sytuacjach wymagających interwencji. Z tego też powodu warto pamiętać o szkoleniach personelu, w tym tych z zakresu cybebezpieczeństwa. Technologia staje się kluczowym sprzymierzeńcem systemów zabezpieczeń. Rozwiązania, w tym te oparte na sztucznej inteligencji, mogą w czasie rzeczywistym analizować obraz, wykrywać nietypowe zachowania czy zmiany w otoczeniu, a następnie podpowiadać najlepsze scenariusze działania. Szczególnie w obiektach wielkopowierzchniowych znacząco przyspiesza to proces oceny sytuacji i skraca czas reakcji.

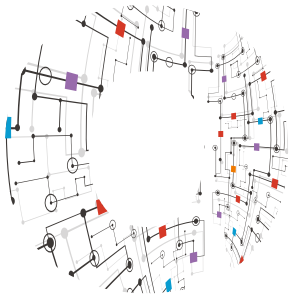
Dzięki harmonijnemu połączeniu kompetencji ludzi i możliwości nowoczesnych systemów bezpieczeństwo w hotelach zyskuje nową jakość – proaktywną, inteligentną i dyskretną, odpowiadającą na potrzeby współczesnych gości.



Samorządy w pułapce CYFROWEGO CHAOSU

Opublikowana przez Najwyższą Izbę Kontroli diagnoza stanu bezpieczeństwa informatycznego samorządów pokazuje, że transformacja cyfrowa zamiast wzmacniać odporność administracji stanowi jej piętę achillesową.

Monika Żuber-Mamakis



Od pierwszych kontrolnych sygnałów o nieskuteczności systemu w 2005 roku po najnowsze alarmy związane z cyberzagrożeniami – tak można ująć historię zarządzania kryzysowego w Polsce, opartą na analizie kolejnych raportów Najwyższej Izby Kontroli (NIK).

Może i dużo formalności, ale za to testów brak

Już w raporcie *Informacja o wynikach kontroli przygotowania administracji zespolonej do działań w sytuacjach kryzysowych* z 2005 roku audytorzy jasno wskazali, że choć procedury zostały spisane na papierze, to *brak regularnych ćwiczeń i symulacji obniżał gotowość operacyjną,* podkreślając potrzebę opartej na praktyce weryfikacji procedur. Kolejna kontrola zatytułowana *NIK o zarządzaniu kryzysowym* z 2011 roku potwierdziła, że *przeciąga się budowa spójnego systemu reagowania na sytuacje kryzysowe,* a rozproszenie zadań w planach cząstkowych znacząco utrudnia komunikację i koordynację.

Od obrony cywilnej do katastrof naturalnych

W 2013 roku NIK porównała polski model obrony cywilnej z doświadczeniami europejskimi w raporcie *Informacja o wynikach kontroli systemów ochrony ludności przed klęskami żywiołowymi* i stwierdziła, że *obecny stan obrony cywilnej uniemożliwia sprawne usuwanie skutków klęsk żywiołowych.* Natomiast w 2019 roku, w opracowaniu *Polska nie ma skutecznego systemu ochrony ludności* audytorzy uznali, że *żaden z 20 skontrolowanych planów nie był rzetelnie przygotowany i kompletny,* co na tle nawałnic sierpniowych 2017 r. obnażyło brak adekwatnych procedur na poziomie lokalnym.

Najnowszy raport Najwyższej Izby Kontroli *Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego* ujawnia niepokojące zaniedbania w 24 badanych urzędach gmin i starostwach powiatowych.

Celem głównym kontroli było zweryfikowanie, czy w 24 jednostkach samorządu terytorialnego (17 urzędów gmin i 7 starostw powiatowych) w okresie od 1 stycznia 2023 r. do zakończenia kontroli prawidłowo, rzetelnie i skutecznie realizowano zadania związane z zapewnieniem bezpieczeństwa informacji oraz zapewnieniem ciągłości działania systemów informatycznych.

Kontrola, przeprowadzona od 1 stycznia 2023 r. do czerwca 2024 r., ujawnia liczne luki organizacyjne i techniczne, które zagrażają bezpieczeństwu danych oraz płynności działania samorządowych systemów IT. Co takiego NIK zarzuca samorządom? Przede wszystkim:

Brak spójnej polityki i nieaktualne standardy. W aż 33% jednostek nie stworzono lub nie wdrożono Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z normą PN-EN ISO/IEC 27001 i krajowymi przepisami. Kolejne 25% orgaznizacji posiadało dokumentację, ale nie przeprowadzało jej regularnego przeglądu ani aktualizacji. Krytycznym problemem okazał się też brak inwentaryzacji zasobów informacyjnych i określenia poziomów ich ochrony – niedociągnięcia tej wagi odnotowano w 92% badanych urzędów.

Brak planów awaryjnych. Blisko trzy czwarte kontroli wykazało, że 71% jednostek nie opracowało formalnej polityki ciągłości działania. Ponad połowa (54%) nie ma planów odtworzeniowych, a jeśli takie ma, to ich nie testowała, co przekreśla szansę na szybkie przywrócenie krytycznych usług w razie awarii.

Brak ograniczenia dostępu. Problemem jest również nieuporządkowane zarządzanie kontami i uprawnieniami – w 22% urzędów konta pracowników pozostają aktywne po zakończeniu umowy, w 5% przypadków personel może instalować oprogramowanie bez kontroli. Taka swoboda stwarza realne ryzyko nadużyć i wycieków danych.

Brak sensownej ochrony serwerowni. Fizyczne zabezpieczenia serwerowni budzą największe zastrzeżenia: w 83% przypadków brakowało kontroli dostępu, odpowiednich warunków klimatycznych i systemów przeciwpożarowych. Co więcej, tylko 46% badanych instytucji realizowało tworzenie kopii zapasowych zgodnie z harmonogramem, a aż 58% przechowywało je wyłącznie na miejscu, bez dodatkowych lokalizacji awaryjnych.

Brak analiz, audytów i szkoleń. Chociaż 71% urzędów deklaruje przeprowadzanie analiz ryzyka, to tylko 63% wykonuje coroczne audyty bezpieczeństwa, często nierzetelnie. A zaledwie 58% poddaje personel obowiązkowym szkoleniom w zakresie ochrony informacji.

Biorąc pod uwagę skalę i różnorodność stwierdzonych nieprawidłowości, Najwyższa Izba Kontroli wezwała Ministerstwo Cyfryzacji do stałego wsparcia jednostek samorządowych w zakresie wdrażania skutecznych rozwiązań organizacyjnych i technicznych, służących poprawie bezpieczeństwa informacji oraz zapewnieniu nieprzerwanej pracy urzędów. Jednocześnie audytorzy wezwali samorządy, by te:

- opracowały i wdrożyły Systemy Zarządzania Bezpieczeństwem Informacji;
- zadbały o okresowy przegląd i aktualizację wymienionego wyżej systemu;
- ustanowiły politykę ciągłości działania oraz opracowały i wdrożyły plany zapewnienia ciągłości działania urzędów, plany odtworzeniowe oraz dokonywały ich okresowego testowania;
- zadbały o okresowe analizy ryzyka utraty integralności, poufności lub dostępności informacji;
- wdrożyły rozwiązania zapewniające odpowiednie zabezpieczenie serwerowni;
- regularnie testowały kopie zapasowe oraz wprowadziły przechowywanie ich poza miejscem wytworzenia;
- zapewniły raz w roku okresowy audyt z zakresu bezpieczeństwa informacji;
- objęły nadzorem oprogramowanie instalowanego na urządzeniach mobilnych.

Jeśli przyjrzeć się tym zaleceniom, to wyraźnie widać, że są to typowe w wielu firmach zasady związane z cyberbezpieczeństwem.

Najczęściej stwierdzone nieprawidłowości w 24 kontrolowanych jednostkach

Tym bardziej martwi fakt, że w jednostkach samorządu terytorialnego występują takie niedociągnięcia. Bez wdrożenia zaleceń NIK polskie samorządy mogą stanąć przed poważnymi wyzwaniami – od opóźnień w obsłudze mieszkańców po poważne incydenty cyberbezpieczeństwa. Najwyższa Izba Kontroli podkreśla, że gwarantem sprawnej i bezpiecznej administracji jest nie tylko technologia, ale przede wszystkim uporządkowane procesy i kompetentny personel.

Za dużo planów, za mało testów

Analiza raportów NIK z lat 2005–2025 ukazuje nadmierny formalizm, brak koordynacji, niedostatki szkoleniowe i rosnące wyzwania techniczne. Już w pierwszym raporcie z 2005 r. zauważono, że plany tworzone były przede wszystkim wypełnieniem formalnego obowiązku, a dekadę później powrócono do konstatacji, że rozproszenie zadań i brak spójnego systemu łączności utrudnia koordynację (2011). Wreszcie, w 2025 roku po raz kolejny podkreślono, że bez regularnych testów i symulacji nawet najlepiej przygotowany plan pozostaje martwym zapisem.

Realizacja zaleceń NIK wymaga nie tylko aktualizacji dokumentów, ale przede wszystkim wprowadzenia kultury organizacyjnej opartej na praktyce i odpowiedzialności. Konieczne staje się wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji, obowiązkowe coroczne audyty wewnętrzne, szkolenia dla personelu oraz ujednolicenie platform komunikacyjnych między wszystkimi szczeblami administracji. Jak jasno stwierdza raport z 2025 r., wdrożenie polityk ciągłości działania oraz coroczne testy przywracania systemów to warunek poprawy odporności cyfrowej.

Wyzwania, przed jakimi stoi polski system zarządzania kryzysowego, pozostają niezmiennie złożone. Rozwiązanie wymaga synergii formalnych regulacji i ciągłej, praktycznej weryfikacji gotowości reagowania – zwłaszcza w czasach, gdy granice między tradycyjnymi katastrofami a atakami cyfrowymi ulegają zacieraniu. •

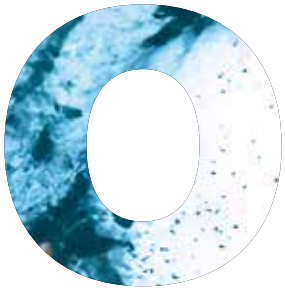
Monika Żuber-Mamakis
Redaktorka „a&s Polska”

Ilustracje: freepik

Płoną góry, płoną lasy...

Najpierw centrum handlowe, potem magazyny, osiedle mieszkaniowe, hala produkcyjna. Siwy dym niesie się nad krajem. Można odnieść wrażenie, że pożarów jest coraz więcej. Szczęśliwie w tym roku lipiec jest wyjątkowo wilgotny, ale tylko patrzeć, jak zaczną płonąć pola i lasy. Pożarów jakby coraz więcej. Przypadek?

Monika Żuber-Mamakis



Ogień nie wybiera, ale czy na pewno? Od rosyjskiej inwazji na Ukrainę w 2022 roku opinia publiczna coraz częściej łączy serię zdarzeń z możliwymi aktami sabotażu. Do tego dochodzą powracające wątpliwości, czy część z tych zdarzeń nie ma także tła, można by rzec, ekonomicznego. Gospodarcze zawirowania czasami skłaniają do desperackich kroków.

Dane statystyczne robią wrażenie, ale nie przynoszą jednoznacznej odpowiedzi na pytanie: Czy pożarów jest więcej, czy mniej? Media robią swoje, bo pożoga to zawsze nośny temat, szczególnie w sezonie ogórkowym. Można jeszcze dodatkowo rozgrzać, nomen omen, atmosferę, sugerując, że każde takie wydarzenie to sabotaż. Faktem jest jednak, że w 2022 roku nastąpił skokowy wzrost pożarów, ale potem ich liczba zmalała. Faktem jest też, że służby poinformowały o zatrzymaniach osób podejrzanych o współpracę z rosyjskim wywiadem. Faktem jest też, że firmy ubezpieczeniowe donoszą o tysiącach wykrytych prób wyłudzeń.

Statystyki opublikowane przez Państwową Straż Pożarną na jej oficjalnym koncie na FB, dotyczące lat 2021–2025 pokazują, że ogólna liczba pożarów w Polsce znacząco się wahała, a najwyższy ich poziom odnotowano w 2022 roku (93 453 zdarzenia), co oznacza wzrost o ponad 44% w stosunku do 2021 (64 730). W roku 2023 liczba spadła do około 59,7 tys., w 2024 – do 58,6 tys., a w pierwszym półroczu 2025 odnotowano ponowny wzrost (ok. 77 tys. do 13 lipca). Wyraźnie widać zatem skok w 2022 r., ale dane te dotyczą wszystkich pożarów. Zdecydowaną większość stanowiły pożary małe (95% wszystkich zdarzeń) i średnie.

Co do pożarów dużych i bardzo dużych, najbardziej spektakularnych i medialnych, ich liczba była relatywnie niewielka i względnie stabilna. W latach 2021–2025 duże pożary występowały 160–255 razy rocznie, bardzo duże – 37–51 razy rocznie. Łącznie każdego roku odnotowywano od ok. 207 do 305 pożarów dużych lub bardzo dużych. Maksimum (305) przypada na 2022 r., a minimum (207) na 2024 r. (średnia pięcioletnia – 238 zdarzeń). Innymi słowy, rok 2022 przyniósł najwięcej dużych pożarów, ale potem nastąpił spadek, a trend w drugiej połowie okresu był raczej malejący. Jak podkreślono w oficjalnej analizie PSP, „w analizowanym okresie 2021–2025 nie zaobserwowano jednoznacznej tendencji wzrostowej w liczbie pożarów". Miejsce miały głównie wahania sezonowe i roczne, typowe dla warunków klimatycznych i działalności ludzkiej.

Analizy typów obiektów pokazują dodatkowe trendy: spadła liczba pożarów budynków mieszkalnych (z ok. 20,6 tys. w roku 2021 do 16,7 tys. w roku 2024). Te statystyki mogą ulec zmianie, bo do końca 2025 roku jeszcze kilka miesięcy, a za nami już choćby tak tragiczne wydarzenie jak ogień, który strawił praktycznie całe ostatnie piętro dużego budynku mieszkalnego w podwarszawski Ząbkach. Ponad 500 osób straciło dach nad głową. Pożar strawił dużą część budynku, w tym dach, i doprowadził do zniszczenia lub zalania mieszkań na niższych kondygnacjach. Liczba pożarów w obiektach użyteczności publicznej, produkcyjnych czy magazynowych pozostawała względnie stała, a w latach 2023–2025 wystąpiła tendencja spadkowa w porównaniu z 2021–2022. Pożary w lasach i uprawach wzrosły znacząco w 2022 r. (do 4,7 tys. pożarów leśnych i 24,5 tys. pożarów upraw), by następnie spaść i ponownie wzrosnąć w 2025 r. To związane jest raczej z warunkami pogodowymi niż jakimś dodatkowym czynnikiem kryzysowym. Reasumując, statystyki wskazują na gwałtowny wzrost liczby pożarów w 2022 r. (wobec roku poprzedniego) i spadek w kolejnych latach. W szczególności pożarów dużych i bardzo dużych nie było więcej niż w 2021; wręcz odwrotnie – ich liczba była wyższa w 2021 i 2022 niż w 2023–2025. Inny niezależny raport przygotowany przez serwis money.pl pt. *Seria pożarów w Polsce budzi niepokój. Dane rzucają inne światło* również pokazuje, że do połowy 2024 r. zmalała liczba dużych pożarów przemysłowych. W pierwszym półroczu 2024 r. miało miejsce tylko 51 dużych/bardzo dużych pożarów hal produkcyjnych (32 duże, 19 bardzo duże), podczas gdy w analogicznym okresie 2023 było ich 71, a w 2022 nawet 74. Zatem dane PSP i analityków nie potwierdzają wzrostu liczby wielkich pożarów od 2022 r., wręcz przeciwnie, po wyraźnym szczycie w 2022 nastąpił spadek.

"Pali się, moja panno..."

Od roku 2022 media wielokrotnie informowały o „serii pożarów" w Polsce, podsuwając myśl o akcjach dywersyjnych czy sabotażu. Wiele publikacji społecznościowych sugerowało, że za podpalenia mogą odpowiadać ukraińscy najemnicy lub ukraińscy politycy. Organizacja fact-checkingowa Demagog wskazała jednak, że tego rodzaju twierdzenia są niezweryfikowane i często zmanipulowane. Udostępniane w Internecie przekazy o „ukraińskich sabotażystach" są dezinformacją – nie ma na to dowodów. Demagog cytuje oficjalne komunikaty prokuratury, np. po pożarze Centrum Handlowego przy ul. Marywilskiej 44 w Warszawie (12 maja 2024 r.) śledczy jednoznacznie stwierdzili, że był on skutkiem sabotażu Federacji Rosyjskiej. Postawiono wtedy zarzuty dwóm obywatelom Ukrainy współpracującym z osobami z rosyjskiego wywiadu. W przypadku. kwietniowego pożaru wielkopowierzchniowego marketu budowlanego w Warszawie śledztwo wykazało, że market został podpalony, a sprawcą jest obywatel Białorusi, Stepan K., który działał na zlecenie rosyjskiego wywiadu. Przytoczone przypadki pokazują, że za niektórymi medialnie nagłośnionymi pożarami w Polsce rzeczywiście stały obce służby specjalne – co potwierdzają źródła rządowe. Jednak nie za wszystkimi.

Seria poważnych pożarów – od 1 lipca na stacji metra Racławicka w Warszawie, przez 3 lipca w Ząbkach, 13 lipca w Mińsku Mazowieckim, aż po zdarzenie dzień później w Siemianowicach Śląskich – rozpaliła w sieci falę spekulacji i krytyki. Według raportu przygotowanego przez Europejski Kolektyw Analityczny Res Futura aż 53 % internautów uważa, że to efekt sabotażu organizowanego przez obce państwa lub wewnętrzne siły polityczne, a 68 % negatywnie ocenia działania rządu i służb, zarzucając im bierność i PR-owe gesty zamiast konkretnych działań. W odpowiedzi ówczesny szef MSWiA Tomasz Siemoniak zapewnił, że dotychczas „nie ma podstaw, by uznać ostatnie pożary za celowe podpalenia", a każda sprawa od stycznia

2024 r. jest analizowana pod kątem ewentualnych aktów dywersji Z drugiej strony przedstawiciele rządu i służb ostrożnie podchodzą do każdej informacji o pożarze. Podczas konferencji prasowej zorganizowanej 14 lipca przez MSWiA ówczesny minister Tomasz Siemoniak powiedział: *Traktujemy poważnie wszystkie sygnały o pożarach – zwłaszcza tych dużych. Od stycznia 2024 r. mieliśmy do czynienia z kilkunastoma próbami aktów dywersji. W związku z tym każde duże zdarzenie, każdy pożar i każda próba podpalenia jest oceniana z punktu widzenia, czy może być próbą aktu dywersji.* Tomasz Siemoniak poinformował, że służby ściśle analizują każdy większy pożar (np. w Mińsku Mazowieckim czy Ząbkach), ale na tym etapie nie zawsze mogą podawać szczegóły śledztwa. W praktyce oznacza to, że zarówno rząd, jak i służby bezpieczeństwa biorą pod uwagę możliwość sabotażu, ale jednocześnie podkreślają, iż wyjaśnienia przyczyn wypadku wymagają czasu. Tak się niefortunnie złożyło, że podczas konferencji odebrano również najnowszy meldunek dotyczący pożaru w Siemianowicach Śląskich. Do pożaru doszło podczas obsługi maszyny z laserem do cięcia. Media zareagowały błyskawicznie: *Gigantyczny pożar w Siemianowicach Śląskich – dym widać z daleka!* lub *Potężny pożar w Siemianowicach Śląskich. Dym było widać z wielu kilometrów!* – to przykłady typowych nagłówków artykułów na temat tego wydarzenia.

Eksperci zwracają jednak uwagę, że dotychczas nie zaobserwowano statystycznie większej liczby pożarów niż zwykle: były one rozłożone w czasie i raczej odpowiadały naturalnym czynnikom (pogoda, niedbalstwo) niż zorganizowanej akcji wroga. Były oficer wywiadu wojskowego Maciej Korowaj zauważył w wypowiedzi dla serwisu Money.pl, że gdyby pożary faktycznie przekraczały normę, służby już by to widziały i uruchomiły nadzwyczajne środki. Tymczasem dane wskazują, iż seria głośnych pożarów nie koreluje ze wzrostem liczby takich zdarzeń na tle wieloletnim.

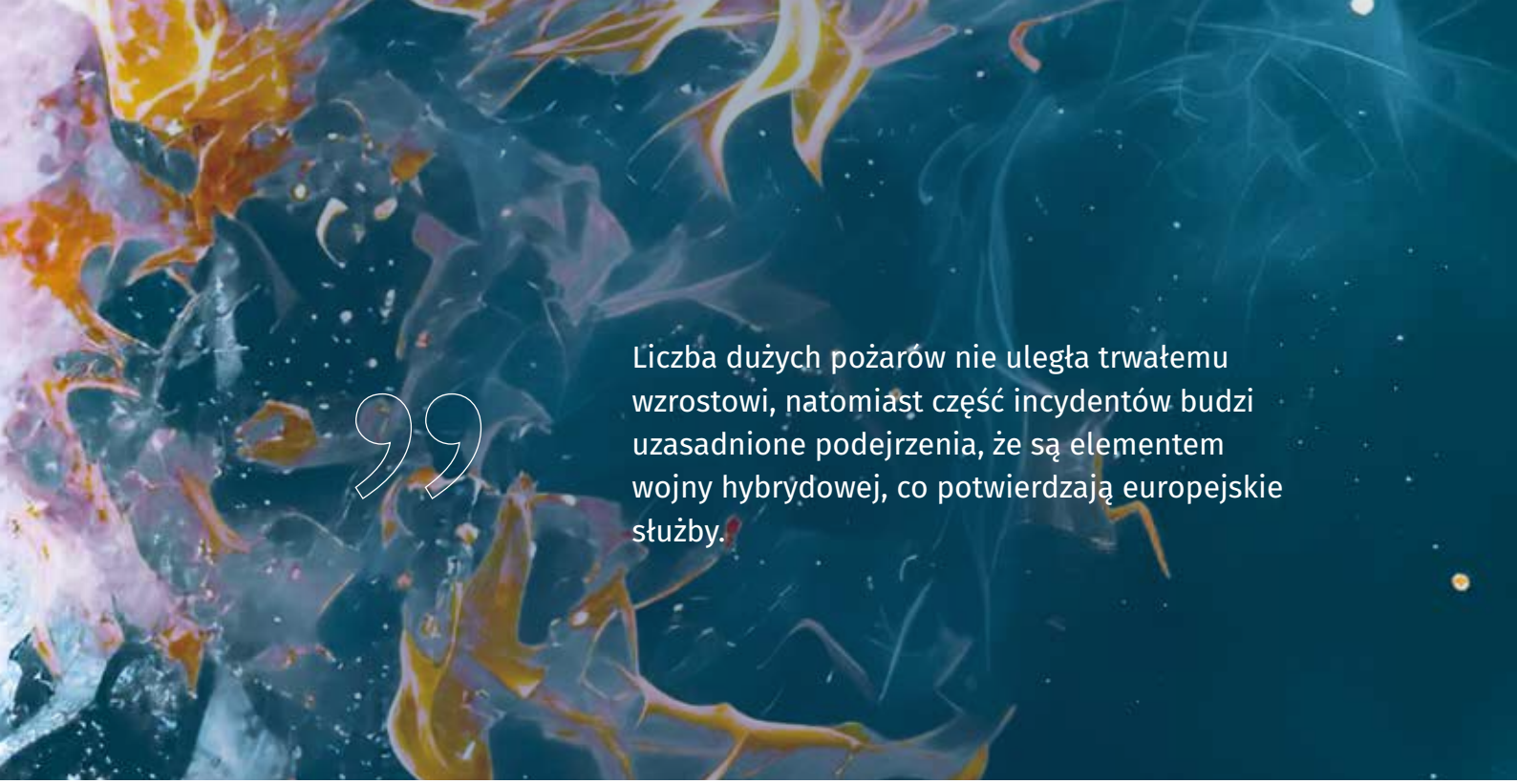
Przypadek, głupota ludzka, determinacja, a może jednak pożary jako element wojny hybrydowej?

Analitycy zwracają uwagę, że kilka spektakularnych zdarzeń, jak choćby wspomniany pożar CH Marywilskiej czy incydenty pakunków wysadzanych w transporcie lotniczym, nosi znamiona zorganizowanej akcji obcych służb. W pierwszym przypadku potwierdziła to polska prokuratura, w drugim prokurator krajowa poinformowała o aresztowaniu czterech osób oraz uznaniu serii podpaleń paczek w Polsce, Niemczech i UK za rodzaj „eksperymentu" w wydaniu GRU. W takich przypadkach motyw polityczny jest ewidentny. Większość pożarów przemysłowych natomiast, zdaniem ekspertów, wynikała raczej z przypadków losowych, wad technicznych czy zwykłego podpalenia kryminalnego, a nie z zaplanowanych działań dywersyjnych. Były oficer wywiadu M. Korowaj, cytowany przez Money.pl, podkreślał, że działania sabotażowe muszą mieć ekonomiczny czy polityczny sens – dotychczas nie ma dowodu, że pojedyncze pożary generowały wymierne straty dla gospodarki Polski, wykraczające poza standardowe statystyki.

Warto też spojrzeć poza Polskę. Od 2022 r. państwa europejskie informowały o licznych incydentach o podobnym charakterze. Poza Polską ataki hybrydowe odnotowano w Litwie, Łotwie, Estonii, Wielkiej Brytanii i Francji – również tam wystąpiły podpalenia i inne akcje sabotażowe podejrzewane jako dzieło rosyjskich służb. Według dziennikarzy międzynarodowej platformy informacyjna Semafor służby wywiadowcze dostrzegły, że rosyjska kampania sabotaży dokonywanych w Europie przybiera na sile, o czym ostrzegają służby wywiadowcze. W Wielkiej Brytanii trzech mężczyzn zostało uznanych za winnych podpalenia magazynu z pomocą dla Ukrainy – prokuratura ustaliła, że operację zleciły rosyjskie służby wywiadowcze. To tylko jeden z ponad 70 podobnych incydentów (pożary, próby wysadzenia ładunków itp.) od czasu inwazji Rosji na Ukrainę w lutym 2022 r., które Associated Press powiązało z Moskwą. Europejscy urzędnicy alarmują, że angażowanie w te działania nieprzeszkolonych sabotażystów znacznie zwiększa ryzyko obrażeń lub ofiar śmiertelnych. Semafor podkreśla, że choć inne kraje (np. Chiny czy Iran) bardziej koncentrują się na cyberatakach, Rosja prowadzi otwartą „wojnę cieni" na terenie państw zachodnich. W 2024 r. zgłoszono aż 12 poważnych aktów podpaleń czy sabotażu (wobec 2 w 2023 r. i żadnego w 2022 r.). W wielu krajach doszło do podpaleń centrów handlowych i magazynów (np. planowane podpalenie centrów handlowych w Polsce, Łotwie i Litwie). Bardzo głośna była też seria „pożarów paczek" w państwach UE – latem 2024 w Polsce, Niemczech i Wielkiej Brytanii płonęły paczki lotnicze z bateriami magnezowymi, co śledczy uznali za test przed ewentualnymi atakami na transport lotniczy. Z kolei w Niemczech w maju 2024 na obrzeżach Berlina doszło do pożaru fabryki Diehl. Lokalne media sugerowały możliwy rosyjski ślad (jak dotąd bez oficjalnych ustaleń). Rozwój wydarzeń w Europie wskazuje zatem na kampanię sabotażową, gdyż ataków o charakterze hybrydowym doświadczyły nie tylko sąsiadujące z Rosją kraje bałtyckie, ale też „stare" państwa NATO. Scenariusz ten potwierdzają zarówno materiały śledcze (np. aresztowania agentów GRU), jak i międzynarodowe raporty wywiadowcze.

„Odbierze asekurację, która mu w czwórnasób pokryje straty..."

W kontekście pożarów często pada pytanie o odszkodowania. Polska Izba Ubezpieczeń informuje, że ubezpieczyciele wypłacili rekordową kwotę 50,3 mld zł odszkodowań w 2024 r., czyli o 6,1 mld więcej niż rok wcześniej. Wypłaty z ubezpieczeń majątkowych (np. domów, firm, komunikacyjnych) wyniosły 33,9 mld zł (wzrost +21,2% r/r), a z polis przeciwpowodziowych i żywiołowych



> Liczba dużych pożarów nie uległa trwałemu wzrostowi, natomiast część incydentów budzi uzasadnione podejrzenia, że są elementem wojny hybrydowej, co potwierdzają europejskie służby.

– 3,7 mld zł (aż +64,1% r/r). Choć raport *Ubezpieczenia w liczbach 2.0* nie podaje osobno sumy odszkodowań tylko za pożary (łączy je z innymi katastrofami), wskazuje to na znaczący wzrost wypłat związanych z żywiołami i powodziami. W konkretnych przypadkach, takich jak tegoroczny lipcowy pożar osiedla w Ząbkach, PIU podała, że ubezpieczyciele wypłacili poszkodowanym już ok. 8 mln zł zaliczek i odszkodowań. W budynku objętym pożarem było 152 ubezpieczonych lokali, a w likwidację szkód zaangażowano 12 firm ubezpieczeniowych. Jak zaznaczono, te wypłaty są zaliczkami – pełne odszkodowania będą stopniowo wypłacane w miarę likwidacji szkód. Podobne informacje o wypłatach dotyczą wielkich pożarów firm czy hal. Brak konkretnych danych dotyczących odszkodowań tylko za pożary utrudnia oszacowanie ich wielkości oraz sprawdzenie ewentualnego wzrostu. Można jednak stwierdzić, że branża odnotowała istotny wzrost kosztów związanych z katastrofami naturalnymi, ale też wzrosła świadomość mieszkańców (większe sumy ubezpieczeń). Wielkie oburzenie wywołał niegdyś premier Włodzimierz Cimoszewicz, który po Wielkiej Wodzie w 1997 roku, powiedział „trzeba być przezornym, trzeba się ubezpieczać"). Co nie znaczy, że nie miał racji i przynajmniej część naszych rodaków wzięła sobie te słowa do serca.

Jednocześnie polskie firmy ubezpieczeniowe od kilku lat intensywnie walczą z wyłudzeniami. Najnowszy *Raport o przestępczości ubezpieczeniowej PIU* (2024) pokazuje, że wykrywalność oszustw rośnie – choć liczbowa skala wyłudzeń spadła. W 2024 r. polskie towarzystwa zgłosiły ponad 32 tys. wykrytych przypadków oszustw ubezpieczeniowych (spadek o 15% wobec blisko 38 tys. w 2023 r.), ale ich wartość wyniosła aż 675 mln zł w porównaniu do 452 mln zł rok wcześniej. Wykryto przede wszystkim próby wyłudzeń odszkodowań (88% przypadków), a wypłacone nienależnie kwoty stanowiły ok. 12% wartości wszystkich oszustw. Oznacza to, że choć mniej spraw ujawniono liczbowo, przeciętna wartość jednej sprawy wzrosła. Wysokie kwoty pojawiają się w różnych segmentach ubezpieczeniowych. Na przykład w ubezpieczeniach na życie oszustwa związane z fałszowaniem dokumentacji medycznej czy fikcyjnymi zgonami wzrosły o ponad 20% r/r. Jeśli chodzi o pożary, nie ma oficjalnych statystyk wskazujących, jak wiele było przypadków celowego podpalenia dla odszkodowania. Niemniej firmy ubezpieczeniowe podkreślają, że podejmują zaawansowane działania prewencyjne (wywiady, analiza danych, AI), by zapobiegać takim oszukańczym roszczeniom. Na przykład w 2024 r. ruszyły wspólne szkolenia z policją i ABW oraz nowe procedury weryfikacji wszystkich dużych szkód majątkowych. Ile z nich to pomysł z *Ziemi obiecanej,* czyli: *Stał źle w interesach, był zachwiany, jak się u nas mówi, więc żeby się poprawić, urządził pożar fabryki i składów, które były wysoko zaasekurowane w kilku Towarzystwach. Odbierze asekurację, która mu w czwórnasób pokryje straty i będzie kpił sobie ze wszystkiego.* Wiarygodnych danych brak, ale nie można tego wykluczyć.

Emocje warto trzymać na wodzy

Analiza danych pokazuje, że choć luty 2022 r. był wyjątkowy, jeśli chodzi o liczbę pożarów, to utrzymują się one na poziomie sezonowych wahań, a liczba dużych zdarzeń tego typu w kolejnych latach nie wzrosła wyraźnie. Rząd i służby traktują każdy większy pożar z najwyższą ostrożnością, ale dotąd udowodniono sabotaż tylko w nielicznych przypadkach – przy tych o szczególnym ciężarze gatunkowym. W ubezpieczeniach natomiast widać lawinowy wzrost wypłacanych świadczeń, co wynika z podnoszenia sum ubezpieczeń i wzrostu kosztów odbudowy. Jednocześnie rośnie skala wykrywanych wyłudzeń (w 2024 r. wykryto 32 tys. prób wyłudzenia na łączną kwotę 675 mln zł), co sugeruje, że problem oszustw ubezpieczeniowych jest poważny, ale jego bezpośredni związek z omawianą falą pożarów jest trudny do udowodnienia. Ostateczna ocena dynamiki zagrożeń leży w rękach śledczych i ekspertów – analitycy radzą unikać emocji i opierania się na twardych danych. Szczególna ostrożność jest wskazana, gdy powtarzają się opinie o „sabotażu" – trzeba je weryfikować w świetle oficjalnych wyników śledztw. Wnioskiem jest, że sama liczba dużych pożarów nie uległa trwałemu wzrostowi, natomiast część incydentów budzi uzasadnione podejrzenia, że są elementem wojny hybrydowej, co potwierdzają europejskie służby. •

Monika Żuber-Mamakis
redaktorka „a&s Polska"

Ilustracje: freepik

Linc Polska

Nowe kamery serii 35 marki Honeywell – inteligentne, bezpieczne, przystępne cenowo

Seria 35 to zaawansowane kamery charakteryzujące się bardzo korzystnym stosunkiem jakości do ceny, zapewniając optymalne bezpieczeństwo obiektów. Doskonale nadają się do zastosowań zarówno wewnętrznych, jak i zewnętrznych, w tym w przestrzeniach handlowych, biurach, małych i średnich firmach, magazynach, stadionach, na parkingach, a także w sektorze hotelarskim czy w obiektach z branży gier. Dzięki 5-letniej gwarancji i zaufaniu, które budzi firma Honeywell, użytkownik może stworzyć bezpieczniejsze środowisko dla swoich klientów i pracowników na długie lata.

Seria 35 obejmuje 13 nowych modeli zapewniających krystalicznie czysty obraz o rozdzielczości do 12 Mpix w zależności od kamery. Oferują doskonałą widoczność w nocy i przy słabym oświetleniu dzięki promiennikom podczerwieni czy funkcji Dual-Light. Wbudowana analityka usprawnia raportowanie oraz zapewnia zgodności ze standardami bezpieczeństwa. Niektóre kamery oferują szeroki kąt widzenia 360° lub obraz panoramiczny 180° dzięki wbudowanym dwóm przetwornikom i obiektywom (Dual-Sensor). Ponadto są wyposażone w wyjście HDMI oraz dają obraz wizyjny, termowizyjny lub kolorowy 24/7. Wśród nowych modeli są kamery Pin-hole, kamery Dual-Light z dualnym oświetlaczem (światło białe + IR), kamera biskeptralna Dual-Sensor & Dual-Light, bispektralne kamery termowizyjne, kamera „Micro-dome" oraz kamery Fisheye. •

Axis Communications

Kamery wieloprzetwornikowe oparte na sztucznej inteligencji

Firma Axis Communications wprowadza na rynek dwie panoramiczne kamery wieloprzetwornikowe o rozdzielczości poziomej do 10K. Dzięki płynnemu łączeniu wszystkich czterech obrazów zapewniają spójny panoramiczny widok w zakresie 180° umożliwiający pełną orientację w sytuacji. Kamery mają zaszytą sztuczną inteligencję, są również wyposażone w procesor głębokiego uczenia, który umożliwia korzystanie z zaawansowanych funkcji analitycznych.

Kamera panoramiczna AXIS Q4809-PVE zapewnia rozdzielczość 26 Mpix przy 30 kl./s oraz zasięg poziomy 180° i pionowy 45°, co pozwala uzyskać niezwykle wyraźny i szczegółowy obraz. Kamera panoramiczna AXIS Q3839-PVE zapewnia rozdzielczość 29 M pix przy 30 kl./s, zasięg poziomy 180° i pionowy 90°, dzięki czemu daje niezwykle wyraźny obraz bez martwych punktów. Dzięki technologii Axis Forensic WDR urządzenia rejestrują wysokiej jakości obrazy nawet w przypadku występowania jasnych czy ciemnych obszarów w kadrze.

Dzięki procesorowi głębokiego uczenia (DLPU) możliwe jest wykonywanie zaawansowanych analiz na obrzeżach sieci. Kamery wyposażono w preinstalowany moduł AXIS Object Analytics do wykrywania, klasyfikowania, śledzenia i zliczania osób oraz typów pojazdów.

Kamery są wyposażone w Axis Edge Vault, sprzętową platformę cyberbezpieczeństwa, która chroni urządzenie i zabezpiecza poufne informacje przed nieuprawnionym dostępem. Ponadto oferują bezpieczne przechowywanie kluczy z certyfikatem FIPS 140-2 poziom 2, zapewniającym bezpieczne przechowywanie i obsługę kluczy kryptograficznych. •

Hanwha Vision

Modułowa kamera AI z obsługą czterech kanałów do dyskretnego monitoringu

Hanwha Vision wprowadza na rynek modułową kamerę AI oferującą obsługę do czterech kanałów w kompaktowej obudowie, idealną do różnorodnych zastosowań i lokalizacji. To zaawansowane rozwiązanie wielosensorowe zapewnia inteligentny i kompleksowy monitoring w dyskretnej formie.

Urządzenie stworzono z myślą o zastosowaniach wymagających niezauważalnej obecności lub monitoringu ograniczonych przestrzeni – bankomaty, wejścia, lady obsługi. Czterokanałowa kamera modułowa PNM-C20000QB składa się z kompaktowych modułów zawierających przetwornik obrazu i obiektyw, kabla połączeniowego, które są połączone do jednostki głównej odpowiedzialnej za przetwarzanie obrazu i komunikację sieciową. System współpracuje z szeroką gamą akcesoriów Hanwha Vision, w tym z modułami obiektywów 2 i 5 Mpix.

Algorytmy AI wykrywają w czasie rzeczywistym ludzi, twarze, pojazdy i tablice rejestracyjne. System odróżnia istotne obiekty od przypadkowego ruchu w tle, wyzwalając alarmy tylko przy ruchu określonych obiektów. Alerty zdarzeniowe reagują na przekroczenie linii wirtualnej, wtargnięcie do strefy, przebywanie w obszarze oraz ruch kierunkowy.

Rozwiązanie zapewnia cyberbezpieczeństwo na najwyższym poziomie: uwierzytelnianie użytkowników, bezpieczną komunikację, kontrolę dostępu i funkcje audytu. Wbudowany bezpieczny element spełnia standardy FIPS 140-3 Level 3 i CC EAL6+, gwarantując ochronę danych i integralność systemu •


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

BCS

Tworzymy obraz *zgodnie ze sztuką*

bcs.pl

POLSKA MARKA