

Ochrona obwodowa lotnisk za pomocą inteligentnego dozoru wizyjnego

Uwagi dotyczące dostępnych usług i zwrotu z inwestycji

Lipiec 2021

Spis treści

1	Streszczenie	3
2	Wprowadzenie	3
3	Tradycyjne rozwiązania ochrony obwodowej	4
	3.1 Rozwiązania fizyczne	4
	3.2 Detektory wtargnięć na ogrodzeniach i bramach	4
	3.3 Detektory wtargnięć na zewnątrz ogrodzeń	4
4	Odpowiedź na wyzwania związane z ochroną obwodową lotnisk	5
	4.1 Nowe inteligentne rozwiązania dozoru wizyjnego	5
5	Koszty i dostępne usługi	5
	5.1 Ocena i pomiar zwrotu z inwestycji	5
	5.2 Oszacowanie kosztów	6
6	Oferta Axis Communications	6
7	Odnośniki do produktów	7

1 Streszczenie

Tradycyjna ochrona obwodowa lotnisk zazwyczaj składa się z ogrodzeń lub murów, które definiują obwód ochrony i zapobiegają wtargnięciu na teren portu lotniczego. Obwód powinien być także wyposażony w urządzenia do detekcji wtargnięć, które wysyłają alarmy na stanowisko monitorowania. Dostępne rozwiązania z zakresu detekcji na obwodzie i w jego pobliżu obejmują przykładowo detektory drutowe, czujniki mikrofalowe i bariery działające w podczerwieni. Choć mają one swoje zalety, nie są w pełni niezawodne. Jednym problemem jest niewykrywanie niektórych zdarzeń, drugi – równie dokuczliwy – stanowią fałszywe trafienia, które w dłuższej perspektywie mogą prowadzić do całkowitego zignorowania poważnych incydentów.

Połączenie kamer do dozoru wizyjnego oraz oprogramowania do detekcji ruchu poszerzyło zakres i możliwości rozwiązań ochrony obwodowej, umożliwiając przejście od prostej detekcji do złożonej analizy wtargnięć. W zależności od lokalnych przepisów kamer można używać do monitoringu wykraczającego poza fizyczne ogrodzenie obiektu, zyskując dodatkowy bufor dozoru i dając operatorowi więcej czasu na reakcję.

W ostatnich latach technologia termowizyjna zrobiła spore postępy, a związane z nią koszty spadły. Kamery termowizyjne połączone z oprogramowaniem do analizy wideo umożliwiają ochronę obiektu przez całą dobę, niezależnie od warunków oświetleniowych. Technologia termowizyjna często dobrze się sprawdza na lotniskach, ponieważ oferuje znakomite możliwości detekcji w dużych instalacjach.

W miejscach, gdzie nie jest możliwe zastosowanie technologii termowizyjnej, znakomitą alternatywą może się okazać technologia mikrofalowa (radar), która zapewnia te same korzyści. Radar Axis potrafi rozróżniać cele i umożliwia integrację z kamerami PTZ na potrzeby efektywnego śledzenia celu. Ta technologia może działać w trybie 24/7 z minimalną liczbą fałszywych trafień, zapewniając oszczędności dzięki niższym kosztom prac wyjaśniających oraz pozwalając zmniejszyć liczebność działu ochrony, który może się skoncentrować na rzeczywistych zagrożeniach.

Ocena rozwiązania ochrony obwodowej powinna być odpowiednia i proporcjonalna. Głównym czynnikiem zawsze jest przeciwdziałanie zagrożeniom, ale jednocześnie system musi spełniać wszystkie wymagania prawne.

Wykazanie zwrotu z inwestycji w rozwiązanie bezpieczeństwa to zazwyczaj trudne zadanie ze względu na brak przychodów, które można by porównać z kosztami. Jednak zastosowanie technologii, która ogranicza potrzebę czynności ręcznych, daje bardziej namacalne rezultaty. Dzięki kamerom można także podnieść efektywność operacyjną, na przykład pokazując intruzom na ekranie, że zostały zarejestrowane dane umożliwiające ich identyfikację.

Kamery Axis są wyposażone w zaawansowane funkcje, które podnoszą jakość obrazu, polepszają łączność sprzętową i zapewniają większą kompresję. Zawierają także opracowane przez Axis procesory ARTPEC, dzięki którym rozwiązania do analizy wideo wchodzące w skład systemu ochrony obwodowej mogą działać na brzegu sieci. Ta rozproszona architektura techniczna umożliwia zwiększanie liczby kamer odpowiednio do ewoluujących potrzeb, a jednocześnie eliminuje konieczność inwestowania w scentralizowaną technologię serwerową.

2 Wprowadzenie

Bezpieczeństwo obiektu o znaczeniu krytycznym opiera się na dwóch filarach: projekcie i ochronie. Lotniska zazwyczaj stanowią element infrastruktury krytycznej swoich krajów, dlatego ich władze mają obowiązek ograniczenia ryzyka wtargnięć przez wdrożenie odpowiednich rozwiązań zabezpieczających, które często stanowią element uporządkowanego, warstwowego systemu obejmującego bariery fizyczne, detekcję wtargnięć, kontrolę dostępu i mobilne patrole strażników.

Stosowane środki ochrony zastrzeżonych obszarów lotniska muszą oczywiście uwzględniać zarówno potencjalne zagrożenia, jak i uwarunkowania operacyjne, a szczególnie **służebności** na potrzeby ruchu lotniczego, topografię terenu, szczególne warunki klimatyczne i ograniczenia środowiskowe. W tym dokumencie omówiono wybrane możliwości z zakresu ochrony lotnisk, a także technologie stosowane w dostępnych rozwiązaniach.

3 Tradycyjne rozwiązania ochrony obwodowej

3.1 Rozwiązania fizyczne

Rozwiązania fizyczne często stanowią zasadniczy element „zewnątrznej warstwy” wieloskładnikowego systemu zabezpieczeń obiektu. Zazwyczaj obejmują one ogrodzenie na obwodzie obiektu, często zbudowane z siatki drucianej lub zgrzewanej, w panelach zgrzewanych lub betonowych. W miejscach znajdujących się blisko radiowych urządzeń nawigacyjno-łącznościowych używa się ogrodzeń z materiału niemagnetycznego. Takie ogrodzenia pełnią dwie funkcje: wyraźnie wyznaczają granice portu lotniczego, ale także zniechęcają ludzi i zwierzęta do wtargnięcia na jego teren. Dodatkowo można zastosować takie elementy jak urządzenia zapobiegające wspinaniu się, drogi dojazdowe, urządzenia zapobiegające przekraczaniu, fundamenty i ekrany ogrodzeniowe.

Dla większego bezpieczeństwa obwód obiektu powinien być wyposażony w rozwiązanie do automatycznej detekcji wtargnięć, które w przypadku przekroczenia obwodu wysyła alarm na stanowisko monitorowania, umożliwiając personelowi wyjaśnienie sytuacji.

3.2 Detektory wtargnięć na ogrodzeniach i bramach

Długi obwód obiektu można zabezpieczyć za pomocą różnego rodzaju „detektorów” drutowych, które na bieżąco przekazują alarmy do operatora systemu bezpieczeństwa. Niektórzy dostawcy oferują ogrodzenia wyposażone w rozwiązania do automatycznej detekcji.

Jednak takie rozwiązania nie są w pełni niezawodne i mogą generować fałszywe alarmy, czyli tzw. „fałszywe trafienia”. Do częstych przyczyn fałszywych trafień należą zwierzęta, poruszające się drzewa i inne rośliny oraz złe warunki pogodowe. Bez dozoru wizyjnego jedynym sposobem na zweryfikowanie przyczyny alarmu jest wysłanie personelu na miejsce zdarzenia. Powtarzające się przypadki fałszywych trafień mogą wywołać zniechęcenie wśród pracowników, prowadząc do ignorowania alarmów, a w skrajnej sytuacji nawet do przeoczenia rzeczywistego zagrożenia.

3.3 Detektory wtargnięć na zewnątrz ogrodzeń

Inne detektory wtargnięć, takie jak czujniki mikrofalowe, bariery na podczerwień lub lasery, są rozmieszczone w strategicznych punktach wokół ogrodzenia lotniska. Również w ich przypadku brak ścisłego przestrzegania zasad instalacji może doprowadzić do takich problemów jak fałszywe trafienia oraz ograniczona odległość i wysokość detekcji. W zastosowaniach lotniczych szczególnym problemem może być ochrona obwodowa oparta na urządzeniach radarowych (mikrofalowych), ponieważ mogą one zakłócać działanie istniejących technologii korzystających z tego samego spektrum częstotliwości. Sam ten czynnik często wyklucza stosowanie urządzeń radarowych. Potencjalne problemy powodowane przez te urządzenia można niemal całkowicie wyeliminować przez staranny wybór częstotliwości i ograniczenie mocy (a zatem i skutecznego zasięgu urządzeń).

4 Odpowiedź na wyzwania związane z ochroną obwodową lotnisk

4.1 Nowe inteligentne rozwiązania dozoru wizyjnego

Połączenie kamer do dozoru wizyjnego oraz oprogramowania do detekcji ruchu poszerzyło zakres i możliwości rozwiązań ochrony obwodowej, umożliwiając przejście od prostej detekcji do złożonej analizy wtargnięć.

Dobrym przykładem są kamery termowizyjne (nazywane także termicznymi lub termograficznymi), które w połączeniu z oprogramowaniem do analizy wideo umożliwiają ochronę danego obszaru o dowolnej porze dnia lub nocy, niezależnie od warunków oświetleniowych. Czujniki korzystające z technologii termowizyjnej często dobrze się sprawdzają na lotniskach, ponieważ oferują znakomite możliwości detekcji w dużych instalacjach.

Czujniki termowizyjne tworzą obraz na podstawie promieniowania podczerwonego emitowanego przez takie obiekty jak pojazdy i ludzie oraz potrafią wykrywać aktywność przez całą dobę, nawet z dużej odległości i w niemal każdym (poza najbardziej ekstremalnymi) warunkach pogodowych. W połączeniu z narzędziami do analizy wideo nowoczesne kamery termowizyjne dysponujące wystarczającą mocą obliczeniową potrafią rozróżnić różne rodzaje obiektów-intruzów i mogą powiadamiać operatora na podstawie określonego zbioru warunków (takich jak kierunek, prędkość, osoba i pojazd). Tradycyjne kamery również dają tę możliwość, ale korzystają ze światła widzialnego, a więc mają pewne oczywiste ograniczenia.

W zależności od lokalnych przepisów kamer można używać do monitoringu wykraczającego poza fizyczne ogrodzenie obiektu, zyskując dodatkowy bufor dozoru i dając operatorowi więcej czasu na reakcję. Rozwiązania obejmujące analizę wideo pozwalają wyzwolić alarm po spełnieniu określonych kryteriów, na przykład gdy ktoś podejdzie do ogrodzenia na odległość mniejszą niż 50 metrów, a następnie alarm o wyższym priorytecie, gdy ta sama osoba zbliży się na mniej niż 10 metrów albo będzie przebywać w określonej strefie przez czas przekraczający zadaną wartość progową.

W ostatnich latach technologia termowizyjna zrobiła spore postępy, a związane z nią koszty spadły. Konkurencyjne ceny w połączeniu z charakterystycznym dla rozwiązań termowizyjnych skutecznym monitoringiem na dużą odległość niezależnym od oświetlenia i warunków atmosferycznych sprawiają, że rozwiązania te często są preferowaną technologią kamer wybieraną do detekcji wtargnięć w ramach ochrony obwodowej.

5 Koszty i dostępne usługi

5.1 Ocena i pomiar zwrotu z inwestycji

Tak jak w przypadku każdego środka bezpieczeństwa ocena rozwiązania ochrony obwodowej powinna być odpowiednia i proporcjonalna. Co oczywiste, przede wszystkim należy wziąć pod uwagę potencjalne zagrożenia, które w dzisiejszych międzynarodowych portach lotniczych mogą mieć różną postać – od uczestników protestów po terrorystów – pamiętając jednocześnie, że system musi spełniać obowiązujące wymagania prawne.

Coraz częstszą praktyką jest zintegrowane podejście do bezpieczeństwa, które uwzględnia dane i opinie pochodzące z innych działów, na przykład IT i operacyjnego. Ponadto, co szczególnie ważne na lotniskach, obejmujących duże obszary o ograniczonym dostępie, należy na jak najwcześniejszym etapie włączyć do prac osoby odpowiedzialne za wymogi inżynieryjne. Kiedyś dobrym punktem wyjścia do ochrony obwodowej

były bardziej tradycyjne metody, mające na celu głównie odstraszenie i spowalnianie potencjalnych intruzów. Dopiero po nich stosowano dodatkowe, techniczne systemy detekcji. Jednak obecnie, w dobie coraz ściślejszej integracji różnych metod i systemów, potrzebne jest bardziej przemyślane i całościowe podejście, i to już na wczesnym etapie.

Zazwyczaj bardzo trudno jest wykazać zwrot z inwestycji w rozwiązanie bezpieczeństwa. Głównie wynika to z faktu, że nie ma dochodów (przychodów), które można by porównać z kosztami. Zazwyczaj pracownicy działu ochrony muszą wyjaśnić kolegom z działu finansów koszty różnego rodzaju incydentów związanych z bezpieczeństwem: czy to koszty bezpośrednie związane z utratą/zniszczeniem mienia czy mniej oczywiste, ale równie dotkliwe koszty w postaci pogorszenia wizerunku firmy lub marki.

Istnieje jednak możliwość wykazania bardziej namacalnego zwrotu z inwestycji, zwłaszcza w przypadku technologii, która ogranicza potrzebę czynności ręcznych lub umożliwia przekierowanie pracowników do wykonywania innych zadań. Dobrym przykładem są rozwiązania, które nie tylko alarmują personel o podejrzanym zachowaniu czy wtargnięciu, ale mogą także inicjować zautomatyzowane „miękkie” reakcje, takie jak powiadomienia dźwiękowe lub migające znaki informujące intruza, że został wykryty, i nakazujące mu opuszczenie terenu obiektu.

Jeśli rozwiązanie obejmuje kamery, można zwiększyć jego efektywność przez pokazywanie intruzom, że zostały zarejestrowane dane umożliwiające ich identyfikację. Przykładowo można na ekranie wyświetlić tablicę rejestracyjną pojazdu, a nawet zdjęcie samego intruza. Dopiero gdy te wstępne środki nie dadzą zamierzonego rezultatu, trzeba wysłać pracowników ochrony, aby zajęli się sprawą bezpośrednio. Niewykluczone, że taki etapowy sposób reagowania na alarmy lepiej się sprawdza na zewnątrz chronionego obwodu, ale i tak w pewnym stopniu zmniejsza potrzebę zaangażowania pracowników ochrony, co daje niewątpliwą korzyść w postaci zwolnienia zasobów.

5.2 Oszacowanie kosztów

Kosztorys powinien być oparty na całkowitym koszcie posiadania, który obejmuje wszystkie koszty rozwiązania w całym cyklu jego istnienia, a więc: koszty materiałów i robocizny, koszty badań, koszty instalacji systemu, koszty operacyjne, koszty konserwacji oraz koszty wycofania z eksploatacji i recyklingu. Może to wymagać zmiany podejścia w działach finansów i zaopatrzenia, ponieważ może wystąpić potrzeba realokacji kapitału między kosztami operacyjnymi a nakładami inwestycyjnymi.

6 Oferta Axis Communications

Otwarte podejście firmy Axis do integracji z rozwiązaniami partnerów sprawia, że jej sieciowe kamery termowizyjne w połączeniu ze sprawdzonymi narzędziami do analizy wideo umożliwiają portom lotniczym wdrażanie wysokowydajnych, zintegrowanych rozwiązań ochrony obwodowej, które są zabezpieczone przed cyberatakami i opłacalne w całym okresie eksploatacji systemu.

Na niektórych obszarach, gdzie czujniki termiczne mogą nie być wystarczająco skuteczne, znakomitą alternatywą jest technologia mikrofalowa (radar), która oferuje wiele zalet technologii termowizyjnej. Technologia radarowa Axis umożliwia odróżnianie ludzi od pojazdów, udostępnia informacje o prędkości i kierunku, umożliwia integrację z kamerami PTZ na potrzeby skutecznego śledzenia celu i może działać w dowolnym elemencie warstwowego rozwiązania bezpieczeństwa – nie tylko na obwodzie obiektu. Podobnie jak kamera termowizyjna, radar działa w trybie 24/7 z minimalną liczbą fałszywych trafień i jest nieczuły na typowe czynniki wyzwalające, takie jak cienie, zmiany oświetlenia, małe zwierzęta, krople deszczu, owady, wiatr czy złe warunki pogodowe. Wraz z upływem czasu rosną oszczędności, ponieważ mniejsza liczba fałszywych trafień przekłada się na niższe koszty niepotrzebnych czynności wyjaśniających oraz mniejszą liczebność działu ochrony, który może się skoncentrować na rzeczywistych zagrożeniach.

Od strony technicznej kamery są wyposażone w zaawansowane funkcje: elektroniczną stabilizację obrazu, która kompensuje ruchy o małej i dużej amplitudzie, wiele wejść i wyjść alarmowych umożliwiających podłączanie urządzeń zewnętrznych oraz zaawansowaną funkcję kompresji (Zipstream), która zmniejsza zapotrzebowanie na przepustowość i pamięć masową.

Kamery Axis zawierają także stworzony przez Axis procesor ARTPEC, który oferuje najlepsze możliwości obliczeniowe w branży i umożliwia osadzenie rozwiązań do analizy wideo z zakresu ochrony obwodowej. Kilka kamer może śledzić wiele zdarzeń, do których dochodzi jednocześnie w różnych miejscach. Ta rozproszona architektura techniczna pozwala objąć rozwiązaniem dowolną liczbę kamer, a jednocześnie eliminuje konieczność inwestowania w scentralizowaną technologię serwerową.

Wykrywane są cztery rodzaje zdarzeń dotyczących jednej lub kilku osób albo pojazdów:

- nieupoważnione wejście lub wjazd (wtargnięcie) na zdefiniowany obszar
- przechodzenie lub przejeżdżanie przez strefy w zdefiniowanej kolejności i zdefiniowanym kierunku
- warunkowe przechodzenie lub przejeżdżanie przez strefy
- przedłużająca się obecność

Ponadto kamery termowizyjne Axis współpracują z głośnikami IP, umożliwiając automatyczne emitowanie komunikatów w chwili detekcji i ostrzeganie potencjalnych intruzów.

Wyżej wymienione technologie Axis można bezpośrednio zintegrować z popularnym oprogramowaniem używanym w portach lotniczych (Genetec, Milestone, SeeTec, Prysm itd.).

Aby określić sprzęt potrzebny do opracowania efektywnego rozwiązania ochrony obwodowej i oszacować koszt instalacji, należy przeprowadzić zarówno studium teoretyczne, jak i oględziny lokalne. Axis wspiera integratorów, udostępniając narzędzia projektowe umożliwiające planowanie, projektowanie i instalowanie rozwiązań oraz zarządzanie nimi.

Narzędzia projektowe Axis wzajemnie się uzupełniają i zapewniają wsparcie na każdym etapie inwestycji – od identyfikacji właściwych produktów na podstawie szczegółowych kryteriów przez planowanie obiektów po instalowanie systemów i zarządzanie nimi. Integrator korzystający z narzędzi Axis może realizować projekty płynniej i efektywniej.

Dzięki naszym narzędziom integrator może wybierać odpowiednie produkty i planować zoptymalizowane systemy na podstawie szacunków i sugestii opracowanych pod kątem określonych specyfikacji. Przekłada się to na krótszy czas dostawy właściwego rozwiązania. Narzędzia te umożliwiają nawet dbanie o bezpieczeństwo zainstalowanych systemów, ponieważ oprogramowanie ułatwia instalowanie uaktualnień i poprawek zabezpieczeń.

7 Odnosiniki do produktów

Termowizyjne kamery IP: seria AXIS Q19

www.axis.com/global/fr/products/axis-q19-series

Oprogramowanie analityczne: AXIS Perimeter Defender

www.axis.com/global/fr/products/axis-perimeter-defender

Zewnętrzne głośniki IP: AXIS C3003-E Network Horn Speaker

www.axis.com/global/fr/products/axis-c3003-e

Radar IP

www.axis.com/global/fr/products/axis-d2050-ve

O firmie Axis Communications

Firma Axis wspiera rozwój inteligentnego oraz bezpiecznego świata poprzez tworzenie rozwiązań sieciowych, które dostarczają wiedzę umożliwiającą poprawę bezpieczeństwa i wdrażanie nowych sposobów prowadzenia działalności. Jako lider rynku sieciowych systemów wizyjnych Axis oferuje produkty i usługi z zakresu dozoru wizyjnego i analiz wideo, kontroli dostępu, systemów domofonowych oraz systemów audio. Axis zatrudnia ponad 3800 wysoce zaangażowanych pracowników w ponad 50 krajach i współpracuje z partnerami na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma Axis została założona w 1984 roku i ma siedzibę w Lundzie w Szwecji.

Więcej informacji o firmie Axis można znaleźć na stronie internetowej firmy pod adresem axis.com.