OCHRONA i BEZPIECZEŃSTWO OBIEKTÓW I BIZNESU

Nr 5/2022 wrzesień/październik
Cena 15,00 (w tym 8% VAT), ISSN 2658-1779, nr ind. 381756

ISSN 2658-1779 10
9 772658 177205

dialtech

CENTRALNY SYSTEM TELEFONII DLA OSADZONYCH
ROZWIĄZANIA DLA SŁUŻBY WIĘZIENNEJ

NAJLEPSZA JAKOŚĆ POŁĄCZEŃ
BŁYSKAWICZNY SERWIS

Lider w telefonii dla osadzonych obecny w 90% okręgów.

Innowacyjny system blokujący pokoje telekonferencyjne.

Firma ponosi 100% kosztów montażu systemu realizacji połączeń.

789 044 432 KONTAKT@DIALTECH.PL WWW.DIALTECH.PL

10 **Jak polskie miasta wykorzystują innowacyjne rozwiązania, by zapewnić bezpieczeństwo mieszkańcom?**
– Sergiusz Parszowski

16 **Ostrzeganie o zagrożeniach w obiektach budowlanych**
– Urszula Garlińska, Michał Pietrzak, Tomasz Sowa

28 **Zastosowanie dronów (BSP) w ochronie osób i mienia**
– Małgorzata Żmigrodzka, Marek Kustra

IFTER®

EQU - RPV01

Wysokiej klasy rejestrator CCTV

TECHNOLOGIA

Rozbudowane możliwości analityczne m.in. analiza profili według płci, wieku, pojazdu oraz innych kryteriów. Identyfikacja i klasyfikacja osób. Zliczanie osób, wyznaczanie kierunku osób i pojazdów. Wykrywanie pozostawionych przedmiotów itp.

PRYNTEC

Rejestratory Digipryn znalazły zastosowanie w ponad jednej trzeciej banków we Francji oraz w wielu centrach handlowych, obiektach rządowych, przemysłowych czy też uniwersytetach. Ponad 50 tys. rejestratorów w ponad 20 krajach świata.

INNOWACYJNOŚĆ

Obsługa dowolnego typu kamer w różnych systemach transmisji danych zarówno w zakresie pobierania strumienia wideo jak i sterowania kamerami PTZ. Ciągłe dostosowywanie do potrzeb klienta pozwala na tworzenie użytecznych i łatwych w obsłudze nowych funkcji.

EFEKTYWNY KOSZTOWO

Koszt licencji uzależniony jest od ilości obsługiwanych kamer dzięki czemu łatwo jest je skalować, zwiększając tym samym efektywność ekonomiczną tego rozwiązania. Bazowa wersja bardzo dobrze wyposażona. Bardzo duża ilość dodatkowych modułów pozwalająca na dostosowanie do potrzeb klienta.

ELASTYCZNOŚĆ

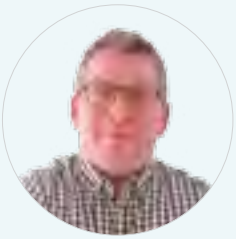
Zarządzanie przez serwer do 10 tys. rejestratorów Digipryn.
Pobieranie obrazu online oraz archiwalnego z dowolnego rejestratora.
Wykonywanie oraz wysyłanie raportów.
W głównym centrum może być wyświetlanych przez jeden komputer do 100 kamer, każda z innej lokalizacji.

INTERAKTYWNY

Odtwarzanie obrazu w
- aplikacji
- komputerze
- smartfonie
- przeglądarce internetowej

Intuicyjne zarządzanie prezentacją wideo, wspierane przez wirtualne joysticki.

MADE IN FRANCE



Drodzy Czytelnicy!

Przed Wami kolejny – piąty już – numer OiB. Numer obfitujący w wiele ciekawych artykułów poruszających będące na topie tematy z branży ochrony i bezpieczeństwa. Dziś m.in. oferujemy „dużą garść" informacji dotyczących funkcjonowania „smart city". Każdego z Was z pewnością zainteresuje materiał poruszający zagadnienia bezpieczeństwa w garażach podziemnych, których mamy w naszym otoczeniu coraz więcej.

Ochrona osób i mienia często kojarzy się wyłącznie z ochroną fizyczną wraz z dodatkowymi zabezpieczeniami elektronicznymi – czy to jednak wszystko? Okazuje się, że nie – bowiem do tego typu ochrony coraz częściej wykorzystuje się drony. Jakie pełnią funkcje i jakie realizują zadania możemy przeczytać w artykule „Zastosowanie dronów (BSP) w ochronie osób i mienia". Przytoczone powyżej artykuły oraz wiele innych zawartych w tym wydaniu OiB stanowią o jego merytorycznej sile. Jak zwykle gwarantujemy wysoką jakość tekstów wynikającą z wiedzy i fachowości naszych Autorów. Wierzymy, że prezentowany numer OiB spełni Państwa oczekiwania i każdy znajdzie w nim coś ciekawego dla siebie.

Robert Gabrysiak
Redaktor prowadzący

AKTUALNOŚCI I INFORMACJE BRANŻOWE

3 **IX edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy – relacja ze spotkania w Hotelu Windsor w Jachrance**

4 **20 lat tradycji i zaufania branży niskich prądów, czyli podsumowanie jubileuszowej edycji Spotkania Projektantów Instalacji Niskoprądowych – relacja z Białki Tatrzańskiej w Termach BANIA**

6 **RCP Master 4 Web Zarządzanie czasem pracy z poziomu przeglądarki internetowej wg aplikacji marki ROGER**

6 **Super panoramiczna kamera 4K od SUMY Solutions**

NOWE TECHNOLOGIE

NOWOCZESNE TECHNOLOGIE KONTROLI DOSTĘPU

8 **Nowoczesne systemy KD**
[Robert Gabrysiak]

SMART CITY

10 **Jak polskie miasta wykorzystują innowacyjne rozwiązania, by zapewnić bezpieczeństwo mieszkańcom?**
[Sergiusz Parszowski]

SYSTEMY DSO

20 **Systemy DSO z funkcją komentatora w halach sportowych**
[Krzysztof Młudzik]

ZARZĄDZANIE

ANALITYKA OBRAZU

14 **Analityka obrazu w branży systemów bezpieczeństwa**
[Robert Gabrysiak]

INTELIGENTNE SYSTEMY ALARMOWE

24 **Inteligentna wtyczka – automatyka budynkowa w systemie alarmowym**
[SATEL]

SYSTEMY BEZPIECZEŃSTWA

40 **Kompleksowe systemy bezpieczeństwa w oparciu o IFTER EQU2**
[Jerzy Taczalski z firmy IFTER]

BEZPIECZEŃSTWO

ZARZĄDZANIE BEZPIECZEŃSTWEM W OBIEKTACH BUDOWLANYCH

16 **Ostrzeganie o zagrożeniach w budynkach budowlanych**
[Urszula Garlińska, Michał Pietrzak, Tomasz Sowa]

DRONY W OCHRONIE OSÓB I MIENIA

28 **Zastosowanie dronów (BSP) w ochronie osób i mienia**
[Małgorzata Żmigrodzka, Marek Kustra]

SYSTEMY DETEKCJI W GARAŻACH PODZIEMNYCH

31 **Systemy bezpieczeństwa w garażach podziemnych**
[Damian Żabicki]

CYBERBEZPIECZEŃSTWO

34 **Anatomia ataków cybernetycznych**
[Grzegorz Data]

44 **OD WYDAWCY**

Dwumiesięcznik Ochrona i Bezpieczeństwo powstaje we współpracy z

SCHRACK

12–13 października 2022 r.

IX EDYCJA OGÓLNOPOLSKICH DNI ZINTEGROWANYCH SYSTEMÓW BEZPIECZEŃSTWA POŻAROWEGO – SCHRACK SECONET I PARTNERZY

PODSUMOWANIE

W dniach 12–13 października 2022 roku, w Hotelu Windsor w Jachrance, po raz dziewiąty odbyła się kolejna, rekordowa edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. Organizatorzy gościli podczas tego wyjątkowego wydarzenia edukacyjnego przedstawicieli branży systemów bezpieczeństwa: inwestorów, generalnych wykonawców, rzeczoznawców, projektantów, instalatorów oraz pozostałych uczestników rynku. W największym w branży szkoleniu wzięło udział prawie 600 osób!

Ogromne zainteresowanie uczestników potwierdziło sensowność powrotu do organizacji spotkania po dwóch latach przerwy spowodowanej pandemią. Wielokrotnie wyrażano opinię o konieczności organizacji częstszych spotkań merytorycznych i edukacyjnych w branży systemów bezpieczeństwa. Schrack Seconet, jako producent i dostawca zaawansowanych technologicznie rozwiązań, stara się na bieżąco spełniać oczekiwania rynku, dlatego każdego roku przygotowuje wiele nowości – dotyczą one zarówno samej organizacji wydarzenia, sposobów komunikacji z uczestnikami (różnorodne formy przekazu), ale przede wszystkim coraz głębszej, dokładniejszej analizy problemów pojawiających się w trakcie projektowania i realizacji obiektów różnego przeznaczenia.

Podczas dwóch dni spotkań z najlepszymi ekspertami w branży słuchacze zapoznali się z najnowszymi wytycznymi dotyczącymi projektowania, instalacji oraz użytkowania m.in. takich systemów jak: system sygnalizacji pożarowej (w tym ochrona obszarów budowy), system sterowania gaszeniem, system telewizji dozorowej, system kontroli dostępu, systemy detekcji gazów, system integrujący urządzenia przeciwpożarowe (SIUP), system kontroli i tłumienia pożaru samochodu elektrycznego, dźwiękowy system ostrzegawczy, system kontroli rozprzestrzeniania dymu i ciepła, system i urządzenia sterujące oddzieleniami przeciwpożarowymi i innymi instalacjami technicznymi obiektu.

Wsparcie merytoryczne podczas tegorocznej edycji szkolenia zapewnili Partnerzy Merytoryczni: Stowarzyszenie Inżynierów i Techników Pożarnictwa – Izba Rzeczoznawców, Polska Izba Systemów Alarmowych, Instytut Bezpieczeństwa Pożarowego NODEX, PROTECT Tadeusz Cisek i Wspólnicy, PZU LAB. Przedstawiciele tych instytucji wzięli udział zarówno w sesji wykładowej, jak i warsztatowej. Dodatkowo w sesji wykładowej swój referat wygłosił ekspert reprezentujący Centrum Naukowo – Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy.

Patronat Specjalny nad wydarzeniem objął Komitet Bezpieczeństwa Gospodarczej Infrastruktury Krytycznej Krajowej Izby Gospodarczej.

Szkolenia odbywały się równolegle w 13 salach! Warsztaty kończące każdy dzień wydarzenia miały charakter sesji pytań i odpowiedzi oraz wymiany poglądów i odbywały się w formie otwartych paneli dyskusyjnych..

Współorganizatorami tego niezwykle istotnego w branży przedsięwzięcia edukacyjnego są następujący producenci i dystrybutorzy:

BELIMO Siłowniki S.A. – światowy lider w dziedzinie opracowywania, produkcji i sprzedaży urządzeń do energooszczędnych instalacji grzewczych, wentylacji i klimatyzacji. **BKT Elektronik** – producent i dostawca kompleksowych rozwiązań na rzecz branży teleinformatycznej. **C-AIM** – dostawca nowoczesnych technologii – systemów telewizji dozorowej oraz kontroli dostępu, integrujący i dostosowujący istniejące rozwiązania do rzeczywistych potrzeb klienta. **Fire & Gas Detection Technologies Inc. (FGD)** – firma dostarczająca innowacyjne rozwiązania w zakresie wykrywania i analizy płomieni, które zapewniają najwyższy poziom bezpieczeństwa zarówno w obiektach przemysłowych jak i komercyjnych. **GAZEX** – od 33 lat konstruuje, produkuje i propaguje stosowanie detektorów i systemów detekcji gazów. **GEO-KAT** – firma oferująca szereg usług umożliwiających kompleksową realizację projektów w zakresie instalacji niskoprądowych systemów automatyki budynkowej i BMS, instalacji elektrycznych, efektywności energetycznej oraz telekomunikacji. **GRAS** – polska, rodzinna firma zajmująca się od początku działalności (rok 1985) produkcją i dystrybucją sprzętu przeciwpożarowego, ratownictwa oraz BHP. **InGas Sp. z o.o.** – polska firma świadcząca kompleksowe usługi związane z wdrażaniem systemów zabezpieczeń przeciwpożarowych. Specjalizująca się w zakresie stałych urządzeń gaśniczych gazowych. **Nedap Security Management** – światowy lider w obszarze systemów kontroli dostępu. **PARTNER** – jeden z wiodących polskich producentów rozwiązań dla dźwiękowych systemów ostrzegawczych, Public Address i tła muzycznego.

Schrack Seconet Polska, w imieniu swoim oraz wszystkich partnerów tegorocznej edycji Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego, składa serdeczne podziękowania prelegentom, uczestnikom, przedstawicielom instytucji oraz uczelni technicznych, patronom merytorycznym, medialnym i patronowi specjalnemu. Organizatorzy dziękują także partnerom technologicznym za wielotygodniową, wspólną pracę nad całokształtem wydarzenia.

O planach związanych z kolejną, jubileuszową edycją wydarzenia organizatorzy będą informować na bieżąco, wszystkie informacje są dostępne na stronie:

wydarzenia.schrack-seconet.pl

LOCKUS

20 LAT TRADYCJI I ZAUFANIA BRANŻY NISKICH PRĄDÓW, CZYLI PODSUMOWANIE JUBILEUSZOWEJ EDYCJI SPOTKANIA PROJEKTANTÓW INSTALACJI NISKOPRĄDOWYCH!

W dniach 28–29 września 2022 w wyjątkowym obiekcie – Hotelu Bania Thermal &Ski – zlokalizowanym w malowniczym zakątku Polski tuż u podnóża Tatr, w Białce Tatrzańskiej odbyła się 20 edycja Spotkania Projektantów Instalacji Niskoprądowych.

W 20 SPIN uczestniczyło ponad 320 osób – projektantów, producentów, dystrybutorów oraz ekspertów branżowych. Swoje rozwiązania zaprezentowało 36 firm:

Złoci Partnerzy: *BKT Elektronik, Dahua Technology, Dormakaba, Grupa Romi, Impakt z PowerWalker, Roger wraz z Sensor – Online, Robert Bosch, TP – Link, Unicard, ZPAS*

Srebrni Partnerzy: *Aco, NSS/BCS, Emiter, Exclusive Networks Poland wraz z firmami: Samsung i Poly, MiwiUrmet, MicroMade, Molex, Poltel Telecom wraz z Corning Optical Communications, RCS Engineering, Salto Systems, Zettler*

Brązowi Partnerzy: *2N, A+V, Assmann, Axium, BitStream, Ewimar, Novet, Polsound, Intelek/Solarix, Tommex*

Rozwiązania omówione przez Partnerów 20 SPIN obejmowały szeroki wachlarz specjalizacji: od systemów sygnalizacji pożarowej, CCTV, kontroli dostępu, wideodomofonowych, przez systemy zasilania gwarantowanego oraz zarządzania budynkiem, rozwiązania Data Center, sieciowe, jak również profesjonalne rozwiązania multimedialne i integrację systemów.

Złoci Partnerzy oprócz standardowych wykładów poprowadzili także warsztaty w mniejszych grupach. Taka forma przekazu wiedzy została wprowadzona po raz pierwszy na jesiennej edycji 19 SPIN. Z racji bardzo pozytywnego odbioru zarówno przez Partnerów jak i Uczestników, została kontynuowana także na jubileuszowej edycji Spotkania.

Tradycją stały się także panele eksperckie. W tym roku uczestnicy 20 SPIN mogli wysłuchać rzeczoznawcę do spraw zabezpieczeń przeciwpożarowych mgr inż. Edwarda Skiepko z prezentacją na temat*: „Nowe wymagania w zakresie uzgadniania projektów urządzeń przeciwpożarowych i projektów budowlanych”.*

Całość jubileuszu dopełnił wieczorny bankiet i część integracyjna, sprzyjająca efektywnej współpracy między partnerami biznesowymi. Główną atrakcją wieczoru był koncert pod hasłem „Born to be wild” Na scenie wystąpili tacy artyści jak: Wojtek Cugowski, Juan Carlos, Kasia Malenda oraz Kuba Jurzyk wraz z tancerzami z grupy Atelie.

W części oficjalnej wieczoru Organizatorzy docenili zaufanie i długoletnią współpracę z następującymi firmami: **BKT Elektronik, TP-Link oraz Robert Bosch**, jak również ekspertem branżowym **Edwardem Skiepko**.

Dziękujemy za wspólnie spędzony czas i aktywny udział w jubileuszowej edycji wydarzenia 20 SPIN!

Spotkanie Projektantów Instalacji Niskoprądowych to już 20 lat tradycji i zaufania branży niskich prądów. Celem SPIN jest tworzenie warunków sprzyjających współpracy oraz powstawaniu nowych inicjatyw i projektów. Spotkania odbywają się dwa razy w roku. Organizatorzy już dziś zapraszają do udziału w wiosennej edycji SPIN Extra 2023, która odbędzie się w kwietniu 2023.

Szczegóły już wkrótce pojawią się na stronie wydarzenia:
https://spin.lockus.pl/

Zachęcamy do obejrzenia zdjęć ze 20 SPIN:
https://flic.kr/s/aHBqjA9Z25

roger
Intelligence for Building

ROGER

RCP MASTER 4 WEB ZARZĄDZANIE CZASEM PRACY Z POZIOMU PRZEGLĄDARKI INTERNETOWEJ

RCP Master 4 Web to dodatkowy moduł systemu RCP Master 4, który umożliwia pracownikom dostęp do wybranych funkcji systemu RCP za pośrednictwem przeglądarki internetowej.

Pracownik korzystający z RCP Master 4 Web może, bez konieczności komunikacji z działem kadr, wykonać wiele czynności samodzielnie, w szczególności zapoznać się z aktualnym stanem wypracowanego czasu pracy, przejrzeć rejestr zdarzeń, złożyć wniosek o urlop lub zgłosić innego rodzaju absencję.

Moduł RCP Master 4 Web umożliwia pracownikom zdalną rejestrację zdarzeń RCP, w tym rejestrację pracy zdalnej.

Aplikacja RCP Master 4 Web udostępnia zestaw funkcji przeznaczonych dla przełożonych różnego szczebla (kierownicy, brygadziści, liderzy zespołów itp.), którzy zyskują w ten sposób wygodny i szybki sposób orientacji wewnątrz zarządzanej grupy pracowniczej.

Wykorzystanie modułu RCP Master 4 Web jako integralnej części zainstalowanego w przedsiębiorstwie systemu rejestracji czasu pracy ułatwia pracownikom zarządzanie swoim czasem pracy. Ponadto automatyzuje i usprawnia pracę działów HR, eliminując szereg czynności i zadań związanych z obsługą pracownika.

Zarządzanie systemem rejestracji czasem pracy z poziomu przeglądarki internetowej w przedsiębiorstwie, które umożliwia RCP Master 4 Web, może być z powodzeniem wykorzystywane w wielu obszarach biznesowych, takich jak produkcja, logistyka, usługi, sektor komercyjny, sektor publiczny i wiele innych.

www.roger.pl

SUMA

SUPER PANORAMICZNA KAMERA 4K

Sumo 33 lata

W naszych magazynach zagościł nowy model kamery Uniview – IPC8542ER4-DUG – panoramiczna kamera sieciowa 4K Starlight (2x2k). Jej głównym zastosowaniem jest obserwacja parkingów i szerokich przestrzeni miejskich, co wykonuje przy pomocy aż 4 obiektywów, a obraz jest scalony w jedną panoramę o polu widzenia 180 stopni. Ponadto dzięki piątej generacji oświetlaczy IR można za jej pomocą wykryć obiekty do 50 metrów.

W odróżnieniu od innych kamer, IPC8542ER4-DUG może śledzić do 5 osób jednocześnie, przypisując im oddzielne okno podglądu. Posiada przy tym pełny pakiet VCA, m.in.: potrafi wykrywać obiekty, które zostały usunięte ze scenerii lub pozostawione. Wyposażona jest także w analityki do zliczania osób.

Niewątpliwie kamery panoramiczne mają szerokie zastosowanie i są niezastąpione przy monitoringu dużych i obszernych przestrzeni.

Na szczegółową prezentację tego modelu zapraszamy na szkolenie on-line, zapisy i szczegóły na stronie: suma.solutions/expert-szkolenia/.

Więcej informacji na:
suma.solutions

RACS 5 v2

Polski system kontroli dostępu klasy *Enterprise*

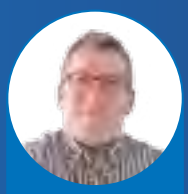
- Rozbudowana wizualizacja wektorowa w nowym module map
- Obsługa systemów rozproszonych terytorialnie
- Integracja z tradycyjnym systemem windowym
- Integracja z serwerowymi systemami windowymi firm KONE, Schindler i innych
- Integracja z systemami SSP, SSWiN, CCTV
- Integracje z platformami zarządzania biurowcami Zonifero, IU Technology, SpaceOS
- Integracje z platformami BMS, VMS, SMS i PSIM
- Integracja z usługą Active Directory
- Rozszerzony moduł obsługi gości

roger

Intelligence for Building

NOWOCZESNE SYSTEMY KD

Gama oferowanych na rynku rozwiązań dotyczących systemów kontroli dostępu jest bardzo szeroka. Wybór odpowiedniego z nich będzie zależał do wielu kwestii i decydował o stopniu zaawansowania technicznego i nowoczesności rozwiązania.



Robert Gabrysiak

Najnowsze osiągnięcia w dziedzinie systemów KD charakteryzują się niezwykłą elastycznością i skalowalnością. Pozwalają łatwo adoptować nowych użytkowników, zwiększać liczbę funkcji, drzwi i lokalizacji. Systemy te można także łatwo integrować z innymi systemami wchodzącymi w skład systemu ochrony. Oczywistym jest że nowoczesne systemy KD to systemy odznaczające się wysokim poziomem bezpieczeństwa oraz bezpieczeństwem przechowywania danych.

Każdy nowoczesny system kontroli dostępu powinien posiadać możliwość optymalizacji pod kątem przyszłych rozwiązań. Ta cecha gwarantuje, że zawsze łatwo możemy zaktualizować system i nie musimy zastępować go innym w przypadku, gdy pojawią się nowe rozwiązania.

Nowoczesny system KD to także technologia oparta na chmurze. Umieszczenie serwera i bazy danych w chmurze daje możliwość bezpiecznego zarządzania danymi i kopiami zapasowymi nawet w przypadku awarii serwera fizycznego. W pewnym sensie daje to korzyści finansowe ponieważ kontrola dostępu oparta na chmurze korzysta z wiedzy ekspertów z tej dziedziny, którzy czuwają nad bezpieczeństwem systemu a jego aktualizacje wykonywane są automatycznie – zatem z obowiązku ich wykonywania zwolnieni są pracownicy działu IT, którzy mogą ten czas przeznaczyć na inne działania. Prawdziwą zaletą rozwiązań chmurowych jest ich skalowalność – w każdym momencie możemy dodać dowolną ilość drzwi oraz uprawnienia nieograniczonej liczbie użytkowników, poświadczanych aplikacją w telefonie komórkowym. Chmura to także natychmiastowy i nieograniczony dostęp do danych – pozwala to na sprawdzenie w czasie rzeczywistym kto i gdzie wchodził oraz o której godzinie dane zdarzenie miało miejsce. Dodatkowo w czasie rzeczywistym możemy otrzymywać powiadomienia o niebezpiecznych zachowaniach (np. próbach naruszenia drzwi). Korzystając

z rozwiązań chmurowych możemy powiedzieć, że system KD przestaje być dodatkowym systemem, którego obsługa powierzona zostaje firmowym informatykom bowiem zarządzanie oprogramowaniem, urządzeniami a także serwerem na którym działa usługa, można pozostawić dostawcy tej usługi jednocześnie przesuwając na niego odpowiedzialność operacyjną na 24h przez cały rok.

Zastąpienie tradycyjnych kart dostępowych urządzeniami mobilnymi takimi jak smartfon to kolejna cecha pozwalająca rozpoznać, że system KD należy do najnowszych rozwiązań. Taka opcja zwiększa nie tylko wygodę użytkowników systemu ale ogranicza również wydatki związane z drukowaniem kart i ich późniejszą wymianą na nowe. Poza tym ryzyko zapomnienia zabrania ze sobą smartfonu jest zdecydowanie niższe niż ryzyko zapomnienia zabrania karty dostępowej.

Kolejną bardzo istotną cechą nowoczesnego systemu KD jest jego cyberbezpieczeństwo. Zaawansowane systemy kontroli dostępu fizycznego są zazwyczaj oparte na IP i wspomagane odpowiednim oprogramowaniem stanowiąc w ten sposób część firmowej sieci IT. Oznacza to, że słabo zabezpieczone przed atakami cyberprzestępców umożliwiają łatwe włamanie się do sieci komputerowej i wykradanie danych lub ich modyfikowanie. Każdego dnia pojawiają się nowe cyberzagrożenia, dlatego należy dbać o regularną aktualizację zabezpieczeń systemu.

Powyżej przedstawiono najważniejsze cechy nowoczesnego systemu kontroli dostępu, dzięki którym możemy rozpoznać czy oferowany lub zainstalowany na obiekcie system to nowoczesna oferta. Pamiętajmy, że rozwój systemów KD jest tak dynamiczny, że system zainstalowany nawet rok lub dwa lata temu może okazać się nieaktualny. Po czym zatem poznać, że zainstalowany już system KD jest przestarzały lub niebawem takim się stanie? Jakie cechy systemu bądź objawy działania o tym decydują? Otóż są to:

- problemy w działaniu – usterki których usunięcie zajmuje dużo czasu
- spowolnienie działania systemu, zwolnienia i opóźnienia w aktualizacjach, spowolnione odświeżanie stanu rzeczywistego itp.
- brak wsparcia technicznego ze strony producenta
- brak możliwości rozbudowy systemu
- trudności lub wręcz brak możliwości przygotowania przez serwisantów poprawek do systemu
- brak możliwości integracji systemu KD z innymi systemami ochrony

Jeśli nasz system wykazuje powyższe cechy to należy poważnie zastanowić się nad jego wymianą bowiem nieaktualny system KD to możliwość generowania wielu problemów. Przykładowo jednym z nich może być niezachowanie zgodności z coraz większą liczbą przepisów prawnych, regulacji i zasad co szczególnie może być problematyczne w sektorach o podwyższonych wymaganiach np. finansowym czy chemicznym. Przestarzały system KD utrudnia też pracę ochronie czy pracownikom recepcji a przede wszystkim znacząco podnosi koszty jego użytkowania.

Wybór nowego i jednocześnie nowoczesnego systemu KD powinien być poprzedzony odpowiedziami na kilka istotnych pytań. Mianowicie powinniśmy określić wymagania poszczególnych działów firmy w zakresie kontroli dostępu – inne wymagania postawi nam dział IT, inne HR a jeszcze inne dział produkcji. W tym momencie dowiemy się komu i jakie dostępy przydzielić, jak dobrać system aby nie narażał naszej sieci IT na ataki cyberprzestępców czy też ilu sumarycznie użytkowników będzie korzystało z systemu. W kolejnym kroku należy wybrać zewnętrznego partnera, który dostarczy nam odpowiednią wiedzę na temat bezpieczeństwa systemu i ułatwi wybór właściwego rozwiązania. Warto zawsze przy wyborze systemu KD przewidzieć przyszłe potrzeby i wymogi stawiane tego typu systemom aby w każdej chwili móc dokonać jego rozbudowy czy aktualizacji.

Podsumowując powyższe rozważania – wybierając system KD warto kierować się odpowiedziami na następujące pytania:

- czy system jest łatwy w obsłudze – chodzi głównie o to czy interfejs oprogramowania jest przyjazny oraz intuicyjny?
- czy system ma możliwość integracji z istniejącymi już innymi systemami zamontowanymi na obiekcie (np. CCTV, SSWiN)?
- czy system będzie kompatybilny z użytymi już urządzeniami KD (np. elektronicznymi klamkami)?
- jakie możliwości uwierzytelniania dostępu mają użytkownicy – czy są to smartfony, czy karty zbliżeniowe lub opaski?
- czy system jest skalowalny a więc czy posiada możliwość rozbudowy i powiększania liczby użytkowników oraz chronionych wejść?
- czy system ma możliwość obsługi przez Internet ?
- jakie możliwości raportowania posiada wybrany system?
- w jaki sposób będą wykonywane i instalowane aktualizacje?

Udzielenie odpowiedzi na powyższe pytania ułatwi wybór optymalnego, nowoczesnego, skutecznego i bezpiecznego systemu KD, który sprawdzi się przez wiele lat użytkowania. ■

Robert Gabrysiak

JAK POLSKIE MIASTA WYKORZYSTUJĄ INNOWACYJNE ROZWIĄZANIA, BY ZAPEWNIĆ BEZPIECZEŃSTWO MIESZKAŃCOM?

Sergiusz Parszowski

Jeszcze niedawno rozmawiając o wdrożeniach z zakresu „smart city" najczęściej przywoływane były przykłady zagraniczne, m.in. z takich miast jak Singapur, Helsinki, Zurich, Oslo, Amsterdam czy Seul. Polskie miasta także sięgają po innowacyjne technologie i coraz częściej z powodzeniem wykorzystują je do zarządzania bezpieczeństwem. Zachęcam do zapoznania się z moim subiektywnym przeglądem rozwiązań stosowanych w polskich miastach na rzecz bezpieczeństwa.

Regionalne Centrum Bezpieczeństwa w Olsztynie

RCB to skrót Regionalnego Centrum Bezpieczeństwa w Olsztynie, które wraz z Regionalnym Magazynem Kryzysowym działa od grudnia 2020 roku. Inwestycja została zrealizowana w ramach projektu „Bezpieczny MOF (Miejski Obszar Funkcjonalny)" i powstała na bazie starego budynku jednostki Państwowej Straży Pożarnej. Wspólne centrum zarządzania kryzysowego obsługuje Miasto Olsztyn oraz sześć gmin ościennych na

terenie powiatu olsztyńskiego. Dysponuje ono zintegrowanym systemem monitoringu i ostrzegania o zagrożeniach oraz spójnym systemem łączności zapewniającym wymianę danych i informacji pomiędzy służbami. W ramach projektu powstał także portal i aplikacja mobilna służące dwustronnej komunikacji z mieszkańcami w sprawach bezpieczeństwa. Całość uzupełniają system ostrzegania na akwenach wodnych oraz dwa pojazdy: rozpoznania oraz dowodzenia i łączności.

Miejski System Informacji Przestrzennej w Kielcach

Miejski System Informacji Przestrzennej w Kielcach to zintegrowane środowisko informatyczne rozbudowane systematycznie od 2009 roku. W środowisku tym znajdziemy informacje, dane i mapy o mieście, dane 3D, zdjęcia ukośne i ortofotomapy. Zakres danych i informacji w połączeniu z narzędziami analitycznymi pozwala dokonywać pogłębionych analiz na potrzeby bezpieczeństwa, np. mapy zagrożeń i mapy ryzyka na potrzeby zarządzania kryzysowego czy analizy wpływu działania poszczególnych obiektów (punktów sprzedaży napojów alkoholowych, miejsc rozrywki itp.) na zakłócenia bezpieczeństwa i porządku publicznego. Dzięki modelowi 3D miasta możliwe jest dokonanie najlepszego wyboru dla przyszłych punktów kamerowych miejskiego systemu monitoringu wizyjnego czy syren alarmowych działających w systemie ostrzegania i alarmowania o zagrożeniach. W razie wystąpienia zagrożenia w budynku, przykładowo pożaru, możliwe jest szybkie ustalenie lokalizacji przyłącza gazowego czy najbliższych hydrantów, a także numerów lokali, w których zamieszkują osoby starsze mogące potrzebować pomocy w ewakuacji.

Inteligentny System Monitoringu w Katowicach

Katowicki Inteligentny System Monitoringu i Analizy (KISMiA) to system kamer dostarczających ogromnej ilości obrazów, w którym praca operatora monitoringu wspomagana jest przez tzw. sztuczną inteligencję. Dzięki automatycznej analizie obrazu system wspiera operatorów w rozpoznaniu kilkunastu rodzajów zdarzeń, m.in. pojawienie się lub zniknięcie obiektu, osoba leżąca na ziemi, jazda „pod prąd", nieprawidłowe parkowanie itp. Funkcja rozpoznawania numerów tablic rejestracyjnych pozwala porównywać dokonywane odczyty z bazą danych pojazdów skradzionych. Za pośrednictwem działających w systemie sieci głośników operator może przeprowadzić zdalną interwencję w przypadku niewłaściwego zachowania ze strony ludzi. Dzięki automatycznej analizie obrazu łatwiejsze jest

także przeszukiwanie nagrań i znalezienie interesujących fragmentów dokumentujących konkretne zdarzenia.

Miejskie Centrum Kontaktu 19115 w Warszawie

Miasto Stołeczne Warszawa jako pierwszy samorząd w Polsce stworzyło wspólne centrum kontaktu z mieszkańcami. Warszawa 19115 to nowoczesny system komunikacji składający się z portalu internetowego, aplikacji mobilnej i numeru miejskiej infolinii. Mieszkańcy nie muszą już zastanawiać się, który z urzędów lub która z jednostek samorządowych jest odpowiedzialna za dany obszar życia miasta. Za pośrednictwem jednej platformy można uzyskać informacje w niemalże wszystkich sprawach, zgłosić dostrzeżony problem, poprosić o interwencję miejskie służby czy też zaproponować pomysł na poprawę warunków życia w mieście lub usprawnienie działania miejskich instytucji. W ramach usługi działa także Warszawski System Powiadomień, który pozwala na otrzymywanie powiadomień w sprawach bezpieczeństwa, w tym ostrzeżeń, zarówno w postaci wiadomości SMS lub przez aplikację mobilną.

Chatbot do komunikacji z mieszkańcami we Wrocławiu

Wrocław, podobnie jak Poznań, zaprzągł do komunikacji z mieszkańcami „chatboty". Wirtualny doradca mieszkańca pozwala komunikować się z urzędem 24 godziny na dobę przez 7 dni w tygodniu przez komunikator Messanger oraz przez miejski portal internetowy. W większości przypadków jest to najszybszy sposób wyszukiwania informacji oraz uzyskiwania odpowiedzi na nurtujące pytania. Pierwotnie był on wykorzystywany wyłącznie w celu informowania w sprawach dotyczących wirusa SARS-CoV-2 i epidemii COVID-19. Dodatkowo umożliwiał na zapisanie się na codzienne powiadomienia. Zastosowanie „chatbotu", oprócz zapewnienia mieszkańcom całodobowej i natychmiastowej odpowiedzi, daje korzyści w postaci możliwości obsłużenia ogromnej ilości zapytań w krótkim czasie oraz uwolnienia dużej ilości czasu urzędników. Dzisiaj za pośrednictwem „chatbota" mieszkańcy mogą dowiedzieć się między innymi jak uzyskać zezwolenie na imprezę masową czy jak dokonać zawiadomienia o zgromadzeniu, jak również uzyskać informacje o zagrożeniach oraz dane kontaktowe do właściwych służb, straży, inspekcji.

Inteligentny system inwentaryzacji dróg w Gdyni

Miasto Gdynia znalazło skuteczny i użyteczny sposób na prowadzenie ewidencji dróg oraz przeprowadzanie okresowych kontroli stanu dróg i drogowych obiektów inżynierskich. Inteligentny system inwentaryzacji dróg wykorzystuje skanowanie lasowe, fotorejestrację oraz dane GIS. Dzięki zebranym danym oraz otrzymanemu narzędziu możliwa jest ocena stanu dróg oraz oznakowania pionowego, pomiar wszystkich obiektów w pasie drogowym, wykrywanie bezumownego zajęcia pasa drogowego czy ocena dostępności obiektów oraz przejezdności dróg pod kątem pojazdów uprzywilejowanych. Jest to także narzędzie ułatwiające przeprowadzenie analiz pod kątem bezpieczeństwa ruchu drogowego i w połączeniu z danymi o wypadkach i kolizjach na identyfikację miejsc wymagających priorytetowej przebudowy infrastruktury drogowej.

Inteligentny System Transportowy w Rzeszowie

Rzeszów nie jest oczywiście jedynym polskim miastem, który posiada inteligentny system trans-

portowy (ITS). Jednak niektóre jego cechy i funkcjonalności sprawiają, że naprawdę się wyróżnia. Oprócz głównej funkcji ITSu jakim jest obszarowe sterowanie ruchem obejmuje on również system zarządzania transportem oraz system informacji pasażerskiej. Jako pierwszy w Polsce to właśnie Rzeszów stworzył dla pojazdów uprzywilejowanych system tzw. „zielonej fali", w którym to dane z systemu GPS o lokalizacji pojazdu z włączoną sygnalizacją świetlną i dźwiękową wykorzystywane są do włączania zielonego światła na danych kierunkach jazdy. Zamontowane przy zatokach autobusowych kamery systemu monitoringu przeciwdziałają bezumownemu korzystaniu z przystanków, zaś dynamiczną informację dla uczestników ruchu drogowego zapewniają tablice zmiennej treści. Uzupełnieniem systemu są stacje meteorologiczne oraz stacje monitorujące zanieczyszczenia powietrza.

Zero wypadków śmiertelnych na drogach w Jaworznie

Jaworzno nie ma sobie w Polsce równych jeżeli chodzi o działania na rzecz poprawy bezpieczeństwa ruchu drogowego. W mieście już od 2005 roku konsekwentnie realizowana jest strategia rozwoju transportu w mieście, zaś w 2013 roku przyjęto strategię „Wizja zero", czyli dążenie do tego, by w wypadkach drogowych nie było ofiar śmiertelnych. Od tego czasu Jaworzno już 3 razy mogło się pochwalić okresami wynoszącymi ponad 12-miesięcy, w czasie których nie doszło na ulicach miasta do śmiertelnego wypadku, zaś 27 maja 2022 r. świętowano 500 dni od ostatniego wypadku śmiertelnego. Miastu udało się to osiągnąć przede wszystkim poprzez konsekwentne realizowanie polityki transportowej, rozwój publicznego transportu zbiorowego i przebudowę układu drogowego. Przy każdej inwestycji drogowej infrastrukturę projektuje się w taki sposób, by wymuszała ona na kierowcach spokojną i bezpieczną jazdę, zaś w przypadkach, gdy człowiek popełni jednak błąd, to by infrastruktura wybaczała mu ten błąd, a nie wymierzała najwyższy wymiar kary.

Pionierski system monitorowania wodociągów w Krośnie

Zainstalowany system monitoringu wodociągów pozwala na łatwiejsze wykrywanie awarii i oszczędności. Składa się między innymi z ośmiu tysięcy nakładek na wodomierze, które przesyłają odczyty do serwera, co w połączeniu z urządzeniami monitorującymi na sieci pozwala wykryć wiele awarii i nieszczelności oraz przypadki kradzieży wody. Opracowana została specjalna metodyka wyszukiwania awarii sieci wodociągowej niewidocznych na powierzchni oraz metodyka ograniczania strat wody w sieci wodociągowej. Dodatkowo powstały wzory procesów zasad działania Centralnej Dyspozytorni Wodociągowej, co pozwala podejmować możliwie trafne decyzje w odpowiedzi na zmiany i zdarzenia zachodzące w sieci wodociągowej.

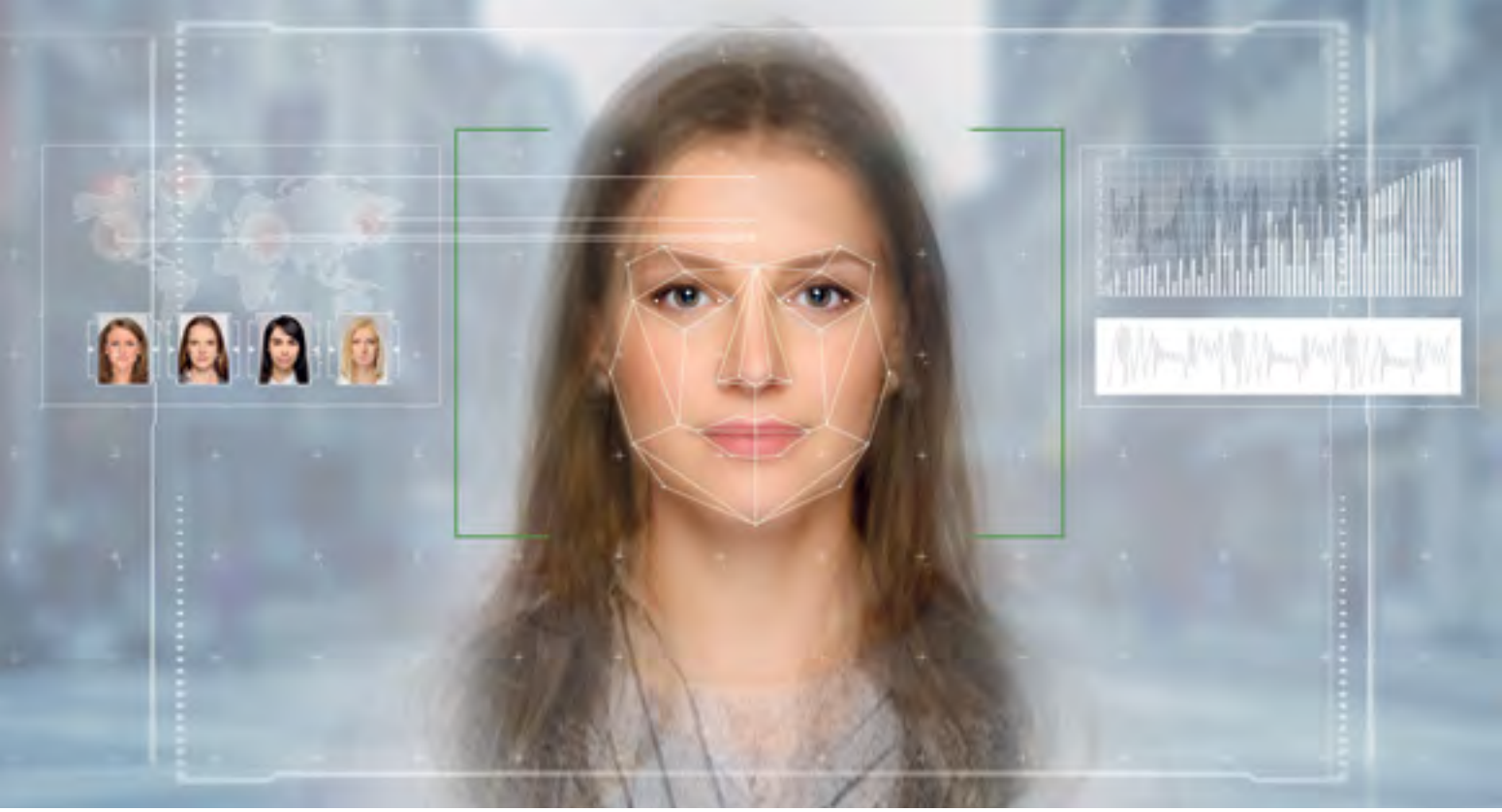
Opaski ratujące życie w Lublinie

W 2019 r. Lublin rozpoczął realizację pilotażowego projektu "SOS dla Seniora", którym objęto 400 seniorów. Wszyscy uczestnicy otrzymali elektroniczne opaski monitorujące całodobowo podstawowe parametry życiowe i za pośrednictwem, których możliwy jest także bezpośredni kontakt z operatorem całodobowego centrum opieki (dwustronne połączenie głosowe). W pilotażu mogły wziąć udział osoby, które ukończyły 60 lat, w szczególności skierowany był on do mieszkańców niepełnosprawnych lub niesamodzielnych, mających trudności w wykonywaniu czynności życia codziennego. Opaski wykonane są z tworzywa sztucznego i posiadają między innymi czujnik tętna, czujnik upadku, czujnik zdjęcia i założenia opaski, przycisk SOS, lokalizator GPS oraz kartę SIM. W Centrum Teleopieki wykwalifikowani ratownicy medyczni i pracownicy techniczni monitorują parametry zdrowotne przesyłane przez urządzenie. Po sukcesie pilotażu projekt jest kontynuowany, a podobne programy realizowane są także w innych miasta i gminach.

Podsumowanie

Wymienione przykłady to oczywiście niejedyne, które zostały w ostatnich latach zaimplementowane przez polskie miasta. Kolejne wdrożenia lub ich pilotaże właśnie trwają. ■

Sergiusz Parszowski
Lider zespołu eksperckiego Instin.pl. Konsultant w sprawach bezpieczeństwa i porządku publicznego, zarządzania kryzysowego oraz bezpieczeństwa osób i obiektów. Audytor i szkoleniowiec.



ANALITYKA OBRAZU W BRANŻY SYSTEMÓW BEZPIECZEŃSTWA

Robert Gabrysiak

Temat analityki obrazu był już poruszany na łamach OiB. Jednakże ciągły rozwój systemów bezpieczeństwa skłonił nas do ponownego wgłębienia się w temat i przedstawienia nowych rozwiązań w tej dziedzinie.

Na początku przypomnijmy sobie czym jest analityka obrazu? Otóż jest to inaczej mówiąc metoda pozyskiwania informacji z zarejestrowanych przez urządzenia monitoringu obrazów. Jednakże to jakie informacje chcemy pozyskać i jak je będziemy przetwarzać definiowane jest przez osoby, które programują, w zależności od potrzeb, urządzenia odpowiedzialne za analitykę obrazu. Dzięki temu możemy zdecydować czy analityka obrazu ma liczyć ludzi, pojazdy, czytać rejestracje pojazdów czy też np. sprawdzać temperaturę. Jednym słowem, analityka obrazu sama automatycznie wskazuje te zagrożenia, które wcześniej zostały zdefiniowane informując o nich np. operatora systemu. W ten sposób system bezpieczeństwa jest niezależny od operatora i jego np. słabszej dyspozycji dnia czy zmęczenia. Przeniesienie analizy obrazu z człowieka na urządzenia odpowiedzialne za analizę obrazu wyklucza z systemu ochrony najsłabsze ogniwo – czyli człowieka. Poza tym narzędzie to – dzięki odpowiednim znacznikom indeksującym – pozwala na łatwe, szybkie i skuteczne przeszukiwanie materiałów archiwalnych ponownie eliminując konieczność wykorzystania do tego celu człowieka. Dobrze skonfigurowana analityka obrazu zapewnia minimalną liczbę fałszywych alarmów – czyli większą skuteczność ochrony.

Współczesna analityka obrazu wykorzystuje sztuczną inteligencję. Ciągły rozwój systemów ochrony oraz analizy obrazów spowodował, że w obszar ten coraz śmielej zaczęła wkraczać sztuczna inteligencja (w skrócie SI lub AI). Wbudowanie sztucznej inteligencji w kamery monitoringu wizyjnego spowodowało, że urządzenia te z elementów pasywnych stały się elementami aktywnymi, które nie tylko obserwują określony teren ale tez wyodrębniają i interpretują (czyli analizują) zarejestrowane dane. Wykorzystanie algorytmów AI w profesjonalnych systemach monitoringu oznacza przede wszystkim nowe możliwości branży ochrony i skrócenie czasu

reakcji na wykryte zagrożenia. Inteligentna analiza obrazu pozwala dziś na realizowanie następujących zadań wykonywanych bezpośrednio przez kamery wyposażone w AI:

- rozróżnianie ruchu wywołanego czynnikami naturalnymi (np. wiatru poruszającego drzewem) od ruchu niepożądanego znacząco obniża liczbę fałszywych alarmów.
- umożliwia realizację zadań tradycyjnej recepcji z zachowaniem pełnej funkcjonalności kontroli dostępu do pomieszczeń, alarmów – tzw. wirtualna recepcja.
- zabezpieczenie prywatności osób widocznych na nagraniach poprzez zakrycie fragmentów obrazu i blokowanie dostępu do nich hasłem.
- możliwość sterowania urządzeniami wejścia/wyjścia poprzez klikanie w nie na obrazie z kamery (np. kliknięcie szlabanu spowoduje jego podniesienie).
- przejęcie nadzoru operatorskiego nad powiadomieniami z systemu PPOŻ – dzięki czemu pracownik ochrony obsługujący system PPOŻ może opuścić miejsce zagrożenia bez konsekwencji.
- wykrywanie pojawienia się ognia przez detektor w kamerze już po zaledwie 30s – gdzie tradycyjny czujnik zareaguje po około 3 minutach.
- detekcja niebezpiecznych zachowań – np. przekroczenia umownej linii (linii bezpieczeństwa na peronie).
- wykrywanie potencjalnego sabotażu – np. próba uszkodzenia kamery, jej zasłonięcia lub zamalowania.
- możliwość śledzenia w tłumie osób podejrzanych – przebywających w określonej strefie powyżej zaprogramowanego czasu.
- śledzenie obiektów w czasie rzeczywistym.
- rozpoznawanie tablic rejestracyjnych.
- wykrywanie kradzieży przedmiotów.

Jak widać, możliwości systemu ochrony wyposażonego w inteligentne urządzenia pozwalające na przeprowadzenie analizy obrazu wg wcześniej zdefiniowanych wymogów, są ogromne. Realizacja powyższych zadań w tradycyjnych nazwijmy „pasywnych" systemach ochrony byłaby praktycznie niemożliwa lub wymagałaby zaangażowania określonej liczby operatorów obserwujących monitory systemu, w zależności od rozproszenia obserwowanego obszaru i próbujących wychwycić każde podejrzane zachowanie lub sytuację.

Zastosowanie sztucznej inteligencji AI w systemach dozoru CCTV staje się coraz bardziej popularne i na pewno będzie rozwijane w najbliższej przyszłości a przyczyna tego jest bardzo prosta – rosnące koszty pracy. Z miesiąca na miesiąc koszty pracy rosną – zatem zatrudnianie do ochrony obiektów dużej liczby osób staje się nieekonomiczne i tu przewagę zdobywają powyżej opisane rozwiązania inteligentnych systemów ochrony.

Systemy monitoringu wizyjnego i ochrony mienia wzbogacone o analitykę obrazu pozwalają zgromadzić wiele informacji i danych z całego systemu. Tutaj pojawia się wyzwanie związane z prawidłowa „obróbką" tych danych (przepisy RODO) oraz problem cyberbezpieczeństwa. Nie wolno bowiem dopuścić do tego aby dane gromadzone przez system bezpieczeństwa dostały się w niepowołane ręce.

Podsumowując można śmiało stwierdzić, że systemy ochrony i bezpieczeństwa wyposażone w inteligentną analizę obrazu to coraz częściej spotykane rozwiązanie i oczywiście absolutna przyszłość. Monitoring wizyjny wzbogacony sztuczną inteligencją to nowość w dziedzinie ochrony rozległych obiektów dający wyższy poziom bezpieczeństwa osób w nich przebywających oraz wyższy poziom zabezpieczenia mienia zarówno w godzinach pracy obiektu jak i poza nimi. Taki monitoring to także nadążanie za współczesnymi zagrożeniami takimi jak epidemie (Covid-19) czy akty terroryzmu. Niebagatelne znaczenie ma też fakt, że systemy ochrony dużych obiektów lub o dużym rozproszeniu, wyposażone w inteligentny monitoring wizyjny to rozwiązania uzasadnione ekonomicznie w odniesieniu do ciągle rosnących kosztów ochrony fizycznej. Dzięki usłudze monitoringu wizyjnego wykorzystującej najnowsze algorytmy do inteligentnej analizy obrazu istnieje możliwość przejęcia większości obowiązków realizowanych dotychczas przez pracowników ochrony stacjonarnej. Zatem nowoczesny system ochrony to system wyposażony w prawidłowo skonfigurowane urządzenia pozwalające dokonywać analizy obrazu, prawnie zgodny z przepisami RODO, odpowiednio zabezpieczony przed cyberatakami oraz skutecznie wykorzystujący zgromadzone dane na potrzeby bezpieczeństwa osób i mienia. ■

Robert Gabrysiak

OSTRZEGANIE O ZAGROŻENIACH W OBIEKTACH BUDOWLANYCH

mgr inż. Urszula Garlińska
mgr inż. Michał Pietrzak
mgr inż. Tomasz Sowa

Zapewnienie warunków do szybkiej i sprawnej ewakuacji jest jednym z podstawowych elementów zapewniających bezpieczeństwo użytkowników w obiektach budowlanych oraz jednym z elementów, który należy wziąć pod uwagę w trakcie projektowania obiektów budowlanych. Istotnym jest wskazanie, że poprzez ewakuację należy rozumieć zorganizowane przemieszczanie się ludzi z miejsc zagrożonych do stref bezpiecznych. Skuteczna organizacja tej ewakuacji jest procesem złożonym, gdzie jej czas zależny jest od wielu czynników związanych zarówno z uwarunkowaniami budowlanymi (tj. rozmieszczeniem i drożnością oraz długością dróg ewakuacyjnych), jak i z działaniami podejmowanymi przez osoby ewakuowane. Strukturę ewakuacji podzielić można na dwa etapy związane odpowiednio z:

- powiadomieniem o wystąpieniu zagrożenia, oraz
- przemieszczeniem się ludzi ze stref zagrożonych do stref bezpiecznych.

Dodatkowo, pierwszy etap można dalej podzielić na kwestie związane ze skutecznym dostarczeniem informacji do odbiorcy oraz prawidłowym odebraniem sygnału, gdzie skuteczne powiadomienie odbiorcy (w kontekście akustycznego przekazywania informacji o zagrożeniu) będzie miało miejsce zawsze wtedy, gdy do użytkownika obiektu będzie docierać fala akustyczna pochodząca ze źródła dźwięku tj. od sygnalizatora akustycznego w systemach sygnalizacji pożarowej, bądź z głośnika w dźwiękowych systemach ostrzegawczych. Natomiast prawidłowe odebranie sygnału zostanie zrealizowane w momencie, gdy wymagania dotyczące słyszalności (a w kontekście sygnalizacji głosowej również zrozumiałości komunikatu) zostaną spełnione. Należy natomiast pamiętać, że w celu spełnienia obu elementów odbiorca musi znajdować się w obszarze pokrycia systemu sygnalizacyjno-alarmowego. Na dzień dzisiejszy najpowszechniejszymi systemami sygnalizacyjno-alarmowymi realizującymi przytoczone powyżej zadania są systemy sygnalizacji pożarowej (SSP) oraz dźwiękowe systemy ostrzegawcze (DSO).

Przekazanie informacji o wykrytym zagrożeniu poprzez systemy sygnalizacji pożarowej realizowane jest automatycznie za pomocą

sygnalizatorów akustycznych lub, w szczególnych przypadkach, sygnalizatorów optycznych. Wykorzystanie tego rozwiązania wiąże się ze stosunkowo niewielkimi kosztami, niemniej system ten daje możliwość nadawania wyłącznie zaprogramowanych sygnałów alarmowych, w związku z czym nie ma możliwości przekazania zmiennych informacji o rodzaju zagrożenia, sposobie postępowania, czy kierunku ewakuacji przez co istnieje prawdopodobieństwo pomylenia alarmów oraz powstania paniki. Problemy te można wyeliminować poprzez zastosowanie dźwiękowego systemu ostrzegawczego (DSO), który umożliwia rozgłaszanie sygnałów ostrzegawczych i komunikatów głosowych nadawanych automatycznie (po otrzymaniu sygnału z systemu sygnalizacji pożarowej) lub przez operatora. Dźwiękowy system ostrzegawczy jest uznawany za najbardziej efektywną metodę zarządzania ewakuacją obiektów, czy to w sytuacjach związanych z zagrożeniem pożarowym, bądź też z innymi sytuacjami powodującymi konieczność sprawnego i szybkiego opuszczenia obiektu przez jego użytkowników. Wynika to z możliwości rozgłaszania przez dźwiękowy system ostrzegawczy zarówno komunikatów wcześniej przygotowanych, jak również nadawanie ich bezpośrednio przez operatora w czasie rzeczywistym. Należy jednak pamiętać, że w obiektach w których zastosowano dźwiękowy system ostrzegawczy zabronione jest stosowanie innych akustycznych urządzeń alarmowych.

Istotnym jest także zdanie sobie sprawy, że skuteczne przekazanie informacji o zagrożeniu nie gwarantuje podjęcia przez użytkownika

odpowiednich działań w sytuacji zagrożenia, a co za tym idzie nie gwarantuje, że ewakuacja obiektu budowlanego przebiegnie zgodnie z założeniami. W związku z powyższym użytkownicy obiektów budowlanych, zwłaszcza wyposażonych tylko w systemy sygnalizacji pożarowej (i towarzyszące im sygnalizacje akustyczne), powinni być poddawani regularnym szkoleniom, aby w sytuacji odebrania informacji o zagrożeniu wiedzieli jakie czynności zobowiązani są podjąć.

Obowiązek stosowania w obiektach budowlanych systemów sygnalizacji pożarowej oraz dźwiękowych systemów ostrzegawczych uregulowany został Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. Nr 109, poz. 719 z późn. zm.), który w § 28 identyfikuje, które obiekty powinny posiadać takie systemy. Dodatkowo przytoczone rozporządzenie identyfikuje obowiązek praktycznego sprawdzania organizacji oraz warunków

Tabela 1. obowiązkowe systemy alarmowania w wybranych obiektach budowlanych

Rodzaj obiektu budowlanego			Obowiązkowy system alarmowania	Realizowanie akustycznego przekazania informacji o zagrożeniu poprzez system
Jednokondygnacyjne budynki handlowe i wystawowe	o powierzchni strefy pożarowej poniżej 5 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I, ZL II, ZL III, ZL IV lub ZL V	Brak wymagań	Brak wymagań
	o powierzchni strefy pożarowej od 5 000 do 8 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I, ZL II, ZL III, ZL IV lub ZL V	SSP	SSP
	zawierające strefę pożarową o powierzchni powyżej 8 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I	SSP, DSO	DSO
	zawierające strefę pożarową o powierzchni powyżej 8 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL II, ZL III, ZL IV lub ZL V	SSP	SSP
Wielokondygnacyjne budynki handlowe i wystawowe	o powierzchni strefy pożarowej poniżej 2 500 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I, ZL II, ZL III, ZL IV lub ZL V	Brak wymagań	Brak wymagań
	o powierzchni strefy pożarowej od 2 500 do 5 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I, ZL II, ZL III, ZL IV lub ZL V	SSP	SSP
	zawierające strefę pożarową o powierzchni powyżej 5 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL I	SSP, DSO	DSO
	zawierające strefę pożarową o powierzchni powyżej 5 000 m^2	zakwalifikowaną do kategorii zagrożenia ludzi: ZL II, ZL III, ZL IV lub ZL V	SSP	SSP
Teatry	o liczbie miejsc poniżej 300		Brak wymagań	Brak wymagań
	o liczbie miejsc od 300 do 600		SSP	SSP
	o liczbie miejsc powyżej 600		SSP, DSO	DSO
Kina	o liczbie miejsc poniżej 600		Brak wymagań	Brak wymagań
	o liczbie miejsc powyżej 600		SSP, DSO	DSO
Sale widowiskowe i sportowe	o liczbie miejsc poniżej 1 500		Brak wymagań	Brak wymagań
	o liczbie miejsc powyżej 1 500		SSP, DSO	DSO
Budynki użyteczności publicznej	Niskie (N)		Brak wymagań	Brak wymagań
	Średniowysokie (SW)		Brak wymagań	Brak wymagań
	Wysokie (W)		SSP, DSO	DSO
	Wysokościowe (WW)		SSP, DSO	DSO
Dworce i porty	przeznaczone do jednoczesnego przebywania poniżej 500 osób		Brak wymagań	Brak wymagań
	przeznaczone do jednoczesnego przebywania powyżej 500 osób		SSP, DSO	DSO
Stacje metra			SSP, DSO	DSO
Stacje kolei podziemnych			SSP, DSO	DSO

Opisy:
ZL I – budynki zawierające pomieszczenia przeznaczone do jednoczesnego przebywania ponad 50 osób niebędących ich stałymi użytkownikami, a nieprzeznaczone przede wszystkim do użytku przez ludzi o ograniczonej zdolności poruszania się,
ZL II – budynki przeznaczone przede wszystkim do użytku przez ludzi o ograniczonej zdolności poruszania się, takie jak szpitale, żłobki, przedszkola, domy dla osób starszych,
ZL III – budynki użyteczności publicznej, niezakwalifikowane do ZL I i ZL II,
ZL IV – budynki mieszkalne,
ZL V – budynki zamieszkania zbiorowego, niezakwalifikowane do ZL I i ZL II,
SSP – system sygnalizacji pożarowej,
DSO – dźwiękowy system ostrzegawczy.

ewakuacji poprzez zapisy w § 17, zobowiązujące właścicieli lub zarządców obiektów, zawierających strefę pożarową przeznaczoną dla ponad 50 osób będących jej stałymi użytkownikami (niezakwalifikowanej do kategorii zagrożenia ludzi ZL IV), do praktycznego sprawdzania co najmniej raz na dwa lata organizacji oraz warunków ewakuacji. Należy także zaznaczyć, że instrukcja bezpieczeństwa pożarowego powinna również zawierać informacje w zakresie warunków i organizacji ewakuacji ludzi uwzględniając identyfikację kierunku ewakuacji oraz wyjść ewakuacyjnych w części graficznej instrukcji. Oczywistym jest, że zaplanowany system organizacji ewakuacji w zakładzie pracy powinien się sprawdzać nie tylko w czasie ćwiczeń ewakuacyjnych, ale także w przypadku realnego zagrożenia, w związku z czym ćwiczenia powinny być dobrane w sposób umożliwiający odwzorowanie rzeczywistych zdarzeń, które mogą wystąpić w obiekcie.

Reasumując, należy zwrócić uwagę na fakt, iż z przedstawionych powyższej wymagań prawnych w zakresie wyposażania obiektów budowlanych w systemy alarmowania wynika, iż każdy obiekt budowlany, w którym wymaga się stosowania dźwiękowego systemu ostrzegawczego wyposażony musi być również w system sygnalizacji pożaru, ale alarmowanie (przekazanie informacji o zagrożeniu do użytkowników obiektu) akustyczne odbywa się tylko i wyłącznie poprzez głośniki dźwiękowego systemu ostrzegawczego. W obiektach, w których dźwiękowy system ostrzegawczy nie został zainstalowany, alarmowanie odbywa się poprzez elementy systemu sygnalizacji pożarowej.

Istotnym jest także fakt, że systemy sygnalizacji pożarowej, jak i dźwiękowe systemy ostrzegawcze, kwalifikowane są do urządzeń pożarowych, w związku z czym projekt, na podstawie którego systemy te mają zostać wykonane musi zostać uzgodniony pod względem ochrony przeciwpożarowej z rzeczoznawcą do spraw zabezpieczeń przeciwpożarowych. Dodatkowo, urządzenia przeciwpożarowe powinny być zaprojektowane zgodnie z obowiązującymi wymaganiami prawnymi oraz zgodnie z zasadami wiedzy technicznej, a oddanie tych systemów do użytkowania musi zostać poprzedzone odpowiednimi próbami i testami. ■

mgr inż. Urszula Garlińska
mgr inż. Michał Pietrzak
mgr inż. Tomasz Sowa

SYSTEMY DSO Z FUNKCJĄ KOMENTATORA W HALACH SPORTOWYCH

Coraz częściej, mając na uwadze chęć optymalizacji kosztów oraz uniknięcie jednoczesnego montażu w jednym budynku dwóch współistniejących systemów dźwiękowych, inwestorzy i projektanci decydują się w przypadku hal sportowych stosować Dźwiękowe Systemy Ostrzegawcze (DSO) w konfiguracji, która pozwala wykorzystywać je również w roli nagłośnienia komentatora sportowego i podstawowego systemu nagłośnienia budynku. Poniższy artykuł naświetla problematykę realizacji tego typu systemów.

Krzysztof Młudzik

Należy zdawać sobie sprawę, że nagłośnienie wielkokubaturowych obiektów sportowych to nie lada wyzwanie. Jak w przypadku każdego obiektu dużej kubatury, kluczowym problemem do rozwiązania będzie zapewnienie odpowiedniego stosunku poziomu ciśnienia akustycznego dźwięku generowanego przez system nagłaśniający, do dźwięku odbitego. Odbicia dźwięku to naturalne zjawisko, które towarzyszy propagacji fali akustycznej w każdym pomieszczeniu. W przypadku hali sportowej, w której dominować będą materiały gładkie i o dużej twardości (np. beton, terakota, blacha trapezowa, szkło) problemem będzie brak tłumienia energii akustycznej. Fale akustyczne w takim pomieszczeniu ulegać będą nakładaniu się i wzmocnieniu, w rezultacie doprowadzając do powstania hałasu pogłosowego. Często zjawisko to będzie dodatkowo potęgowane przez sam kształt hali sportowej – dla przykładu: popularne rozwiązania architektoniczne takie jak sufit w kształcie kopuły, czy też sklepienie w formie łuku prowadzić mogą do ogniskowania fali akustycznej. Rezultatem występowania hałasu pogłosowego będzie znaczne pogorszenie komfortu słuchaczy oraz ograniczenie zrozumiałości mowy reprodukowanej w pomieszczeniu.

W zaistniałej sytuacji projektowanie systemu nagłośnienia, którego specyficznym rodzajem jest przecież system DSO, staje się nierozłącznie powiązane z zagadnieniem adaptacji akustycznej wnętrz. W uproszczeniu – systemowi elektroakustycznemu zapewnić należy właściwe warunki pracy.

W Polsce od kilku lat obowiązuje norma akustyczna PN-B-02151-4:2015-06 „Akustyka budowlana. Ochrona przed hałasem w budynkach. Część 4: Wymagania dotyczące warunków pogłosowych i zrozumiałości mowy w pomieszczeniach oraz wytyczne prowadzenia badań", która określa wymagania odnośnie akustyki obiektów sportowych w kontekście czasu pogłosu. Czas pogłosu (Reverberation Time – RT) to parametr akustyki wnętrz, który opisuje jak długo po zakończeniu pobudzenia pomieszczenia będzie ono wybrzmiewać. Zgodnie z zaleceniami PN-B-02151-4:2015-06 czas pogłosu hali sportowej nie powinien przekraczać: 1,5 sekundy dla obiektów do 5 tys. metrów sześciennych oraz 1,8s dla obiektów większych.

Aby uzyskać powyższy efekt zazwyczaj stosuje się kombinację środków technicznych w po-

staci okładzin akustycznych, paneli dźwiękochłonnych oraz specjalistycznych tynków.

a. Panele akustyczne produkowane są zazwyczaj z wełny mineralnej, lub też sprasowanej słomy drzewnej (dodatkową zaletą tych ostatnich, w kontekście hal sportowych jest odporność na uderzenia mechaniczne). Mogą być one mocowane do powierzchni sufitu hali, lub też na płaskich ścianach. Panele cechują się wysoką skutecznością w tłumieniu dźwięku z zakresu środkowych i wysokich częstotliwości.
b. Duże powierzchnie ścian i sufitu obłożyć można perforowanymi płytami akustycznymi, w połączeniu z wkładem z wełny mineralnej. W zależności od grubości takiej płyty, jej stopnia perforacji oraz użytej wełny (istotnym czynnikiem będzie jej grubość i gęstość) ustrój tego typu może zapewnić pochłanianie oprócz wysokich, także i niskich częstotliwości.
c. Tynk akustyczny to rozwiązanie popularne ze względu na brak potrzeby wykonywania dodatkowych podkonstrukcji, a także możliwość szybkiej jego aplikacji. Jest to jednak rozwiązanie stosunkowo kosztowne. Tynk ma postać piany celulozowej, która natryskiwana jest bezpośrednio na podłoże (np. beton, lub też blachę). Właściwości akustyczne tynku zależeć będą głównie od jego faktury oraz grubości natrysku – satysfakcjonujące efekty pozwala uzyskać zazwyczaj już kilkunastomilimetrowa warstwa.
d. Najtańszym z kolei sprawdzonym rozwiązaniem jest stosowanie wełny mineralnej w formie rolek. Wełna może być mocowana do powierzchni podłoża poprzez klejenie, lub też za pomocą elementów mocujących w postaci linek stalowych, haczyków, płaskowników itp.. Należy mieć jednak na uwadze, że wełna jest stosunkowo mało odporna na uderzenia mechaniczne i ma tendencję do prószenia. Konieczne jest więc jej właściwe zabezpieczenie.

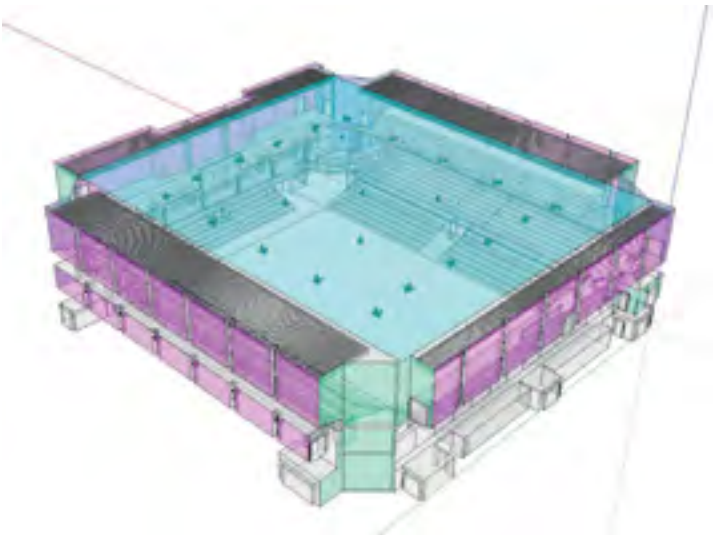
Przemyślane zastosowanie wyżej wymienionych środków pozwala zapanować nad akustyką nagłaśnianego wnętrza, co nie tylko ma wyraźne przełożenie na komfort osób w nim przebywających, ale niejednokrotnie pozwala zmniejszyć ilość (i koszt) sprzętu nagłaśniającego, niezbędnego do nagłośnienia obiektu.

Drugim istotnym problemem do pokonania będzie problem wysokiego poziomu hałasu. Warto zdawać sobie sprawę, że w wielkokubaturowych obiektach sportowych poziom tegoż hałasu może osiągać wartości rzędu 90–95 dB. Źródłem hałasu we wnętrzu hali sportowej będzie publiczność oraz systemy wentylacji mechanicznej, a czynnikiem wzmagającym jego natężenie omawiany we wcześniejszej części artykułu pogłos.

Mając na uwadze potrzebę zapewnienia zrozumiałego przekazu głosowego – zarówno

Rys. 1. Wnętrze hali sportowej w Gdańsku – cała powierzchnia sufitu zasłonięta jest panelami akustycznymi

w kontekście emisji komunikatów alarmowych, ale też w kontekście prowadzenia konferansjerki oraz realizacji imprez sportowych – konieczne jest zapewnienie należytego stosunku poziomu sygnału dźwiękowego wobec poziomu hałasu (tła akustycznego). Zgodnie z dobrym zwyczajem systemy akustyczne projektować należy tak, aby były w stanie zapewnić wspomniany stosunek na poziomie 6–20dB. Z właściwości psychofizjologii słyszenia wynika, że spełnienie powyższego warunku daje duże prawdopodobieństwo, że obecność hałasu nie będzie degradować percepcji dźwięku użytecznego, a tym samym ograniczać zrozumiałości przekazu. W sytuacji gdy system



Przykładowa adaptacja akustyczna hali zrealizowana w oparciu o połączenie:
- akustycznych płyt sufitowych (część centralna)
- akustycznych paneli ściennych (za trybunami i w narożnikach)
- baffli akustycznych (ponad antresolami)

elektroakustyczny nie jest w stanie zapewnić właściwego SNR (Sound-to-Noise Ratio) należy oczekiwać pomniejszonej zrozumiałości mowy, co ma przełożenie na zredukowanie wartości obiektywnego wskaźnika zrozumiałości mowy STIPA, którego pomiar jest jednym z kryteriów odbioru Dźwiękowych Systemów Ostrzegawczych.

Możliwość wygenerowania przez system nagłaśniający komunikatu głosowego z natężeniem przekraczającym 95 dB jest uzależniona od parametrów technicznych zestawów głośnikowych. Poziom ciśnienia akustycznego generowany przez głośnik jest bowiem funkcją jego skuteczności oraz mocy znamionowej. Skuteczność głośnika to parametr, który informuje o tym, jaki poziom natężenia dźwięku jest on w stanie wygenerować przy doprowadzeniu sygnału o określonych parametrach – zazwyczaj przyjmuje się w tym przypadku 1W/1m (w przypadku DSO wykorzystywane jest też pojęcie czułości – definiowane jako poziom jak w pasmie 100 Hz–10 kHz dostarczy głośnik zasilany mocą 1W, w odległości 4m). Poziom emisji dźwięku wzrasta w funkcji mocy dostarczanej do głośnika, przy czym ograniczeniem jest tu moc znamionowa głośnika – rozumiana jako maksymalny poziom mocy z jaką głośnik może pracować długoterminowo bez narażenia się na uszkodzenie oraz przy akceptowalnych zniekształceniach.

Wzór pozwalający oszacować poziom SPL generowany przez głośnik:

$$L_{SPL} = L_E + 10log(P)$$

Gdzie:

L_{SPL} – poziom ciśnienia akustycznego generowany przez głośnik
L_E – skuteczność głośnika
P – moc dostarczana głośnikowi

Z każdym podwojeniem mocy dostarczanej głośnikowi generowany poziom ciśnienia akustycznego wzrasta o 3 dB. Przykład – głośnik tubowy o skuteczności 102 dB, zasilany mocą 4W generuje poziom ciśnienia akustycznego rzędu 102 + 2 x 3 = 108 dB

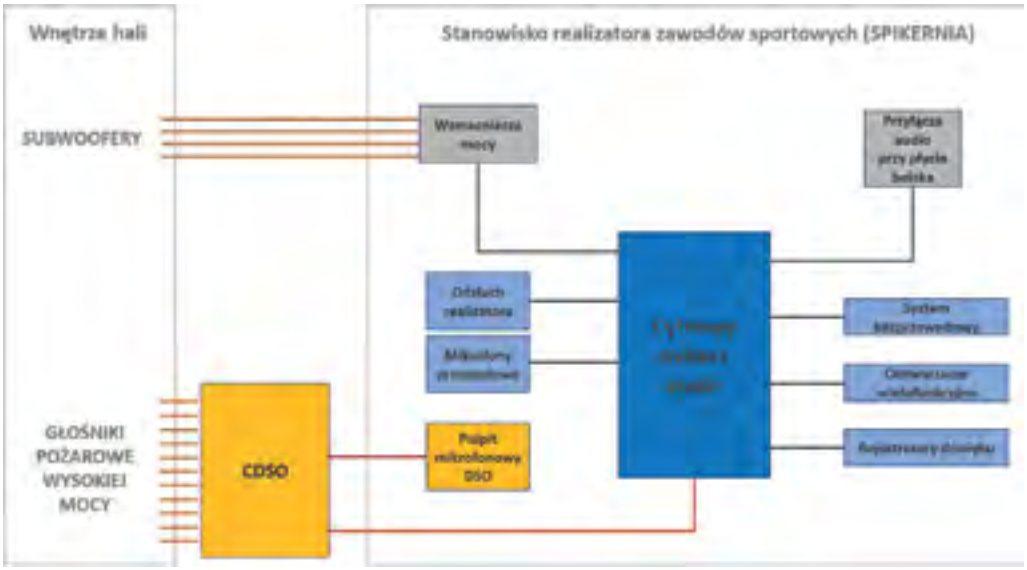
Rys. 2. Porównanie wielkości pożarowego głośnika tubowego o mocy 30W oraz dwudrożnego głośnika tubowego na przykładzie ABT-HP240

Wygenerowanie wysokiego poziomu ciśnienia akustycznego wymaga więc zastosowania głośników cechujących się wysoką sprawnością oraz dużą mocą znamionową. Ze względu na swoją konstrukcję głośniki małego formatu cechują się zazwyczaj niską sprawnością – rzędu 87–92 dB. Wyjątkiem od tej reguły są głośniki tubowe, które skonstruowane są w ten sposób, że emitowany dźwięk promieniowany jest na zewnątrz poprzez rozszerzającą się w regularny sposób tubę. Tuba pełni rolę transformatora zwiększającego impedancję akustyczną obciążającą membranę głośnika, co podnosi kilkukrotnie efektywność przekazywania energii z przetwornika do cechującego się niską gęstością powietrza. Głośniki tubowe mają jednak pewnego rodzaju ograniczenia – w zależności od wielkości i kształtu tuby zmienia się pasmo przenoszenia głośnika i poziom zniekształceń, których obecność jest nieodzowną cechą głośnika tubowego. Warto jednak zdawać sobie sprawę, że im niższe częstotliwości ma przenosić głośnik tubowy, tym większy musi być rozmiar tuby. W przypadku kompaktowych głośników tubowych, o jakich zazwyczaj mowa w kontekście systemów DSO, należy się więc spodziewać, że będą one w stanie przenosić dźwięk wyłącznie w zakresie środkowych i wysokich częstotliwości, a więc w górnej części pasma mowy.

Zgodnie z Rozporządzeniem Ministra Spraw Wewnętrznych. i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. z 2010 Nr 109, poz. 719) sale widowiskowe i sportowe o liczbie miejsc powyżej 1500 powinny być wyposażone w Dźwiękowy System Ostrzegawczy. Funkcja takiego systemu to przede wszystkim funkcja bezpieczeństwa. Odpowiada on za emisję alarmowych komunikatów automatycznych wysterowanych przez Centralę Systemu Sygnalizacji Pożarowej (CSSP) oraz komunikatów wygłaszanych za pośrednictwem konsoli alarmowej – mikrofonu strażaka.

Większości czytelników system DSO kojarzyć się będzie z niewielkich rozmiarów głośnikami pożarowymi. Urządzenia tego typu znakomicie sprawdzają się w standardowych aplikacjach takich jak: budynki użyteczności publicznej, hotele, obiekty handlowe itp.. W przypadku obiektów sportowych, gdzie mieć będziemy do czynienia z dużą wielkością kubatury oraz wysokim poziomem hałasu, rozwiązania te w wielu przypadkach okazują się jednak nieskuteczne.

W systemach DSO dla hal sportowych stosuje się zazwyczaj głośniki tubowe, które pozwalają wygenerować wysoki poziom dźwięku. W przypadku tub małego formatu odbywa się to kosztem pasma przenoszenia oraz zniekształceń – a więc jego jakości i barwy dźwięku. Alternatywnym rozwiązaniem może być w tym przypadku zastosowanie dużego formatu głośników tubowych o konstrukcji dwudrożnej. Głośniki te będą



Rys. 3. Schemat ideowy systemu

posiadały dedykowany komponent niskotonowy (zazwyczaj o średnicy od 8 do 15 cali) oraz osobny komponent wysokotonowy, zamknięte we wspólnej obudowie, której wielkość umożliwiać będzie przenoszenie tonów niskich. Istotną zaletą tego typu rozwiązania jest możliwość wykorzystania tego samego systemu głośnikowego zarówno do realizacji celów związanych z reprodukcją komunikatów głosowych, jak i w celach muzycznych.

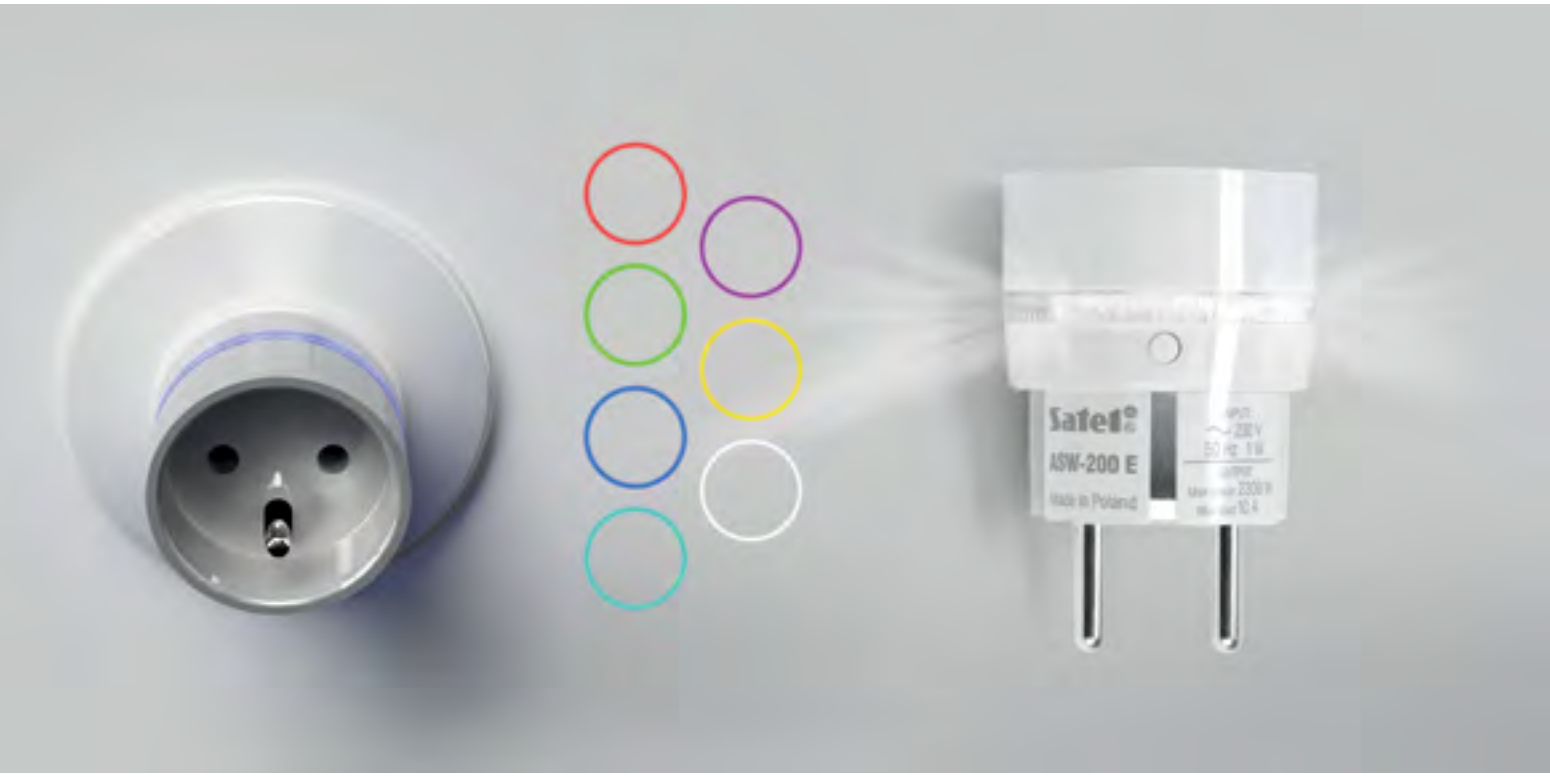
Aby uzyskać powyższą funkcjonalność, w tego typu systemach konieczne jest, aby CDSO zintegrować z systemem komentatora sportowego. System ten zbudowany jest z szeregu źródeł dźwięku – wliczając mikrofony przewodowe, bezprzewodowe oraz różnego rodzaju odtwarzacze oraz odsłuchu realizatora (w formie monitorów odsłuchowych i/lub słuchawek) podłączonych do miksera dźwięku współpracującego z procesorem audio, lub też miksera cyfrowego łączącego w sobie funkcję obu powyższych. Wspomniany mikser, lub też procesor dźwięku, dostarcza do CDSO liniowe sygnały audio, które wprowadzone są na wejście audio opatrzone niskim poziomem priorytetu. Wejście to jest routowane na strefy we wnętrzu hali sportowej, a zazwyczaj również na wybrane strefy komunikacji dostępne kibicom oraz strefy zaplecza. Co istotne, wspomniane wejście jest dezaktywowane na czas alarmu, co pozwala zrealizować wymóg, aby system DSO po przejściu w stan alarmowy stawał się niezdolny do realizacji funkcji niezwiązanych z rozgłaszaniem komunikatów alarmowych.

Mając na uwadze funkcjonalność systemu, na stanowisku realizatora zawodów projektuje się również rozwiązanie w postaci pulpitu strefowego, który w przypadku szeregu nieprzewidzianych sytuacji związanych z realizacją imprez masowych umożliwi spikerowi ręczne rozgłaszanie komunikatów do wybranych stref budynku, lub też wyzwalanie z pamięci systemu DSO komunikatów automatycznych (np. wezwanie do zachowania spokoju na trybunach).

W przypadku obiektów o podwyższonym standardzie możliwości systemu w zakresie reprodukcji tonów niskich będą dodatkowo poszerzone poprzez zastosowanie głośników typu subwoofer, które zasilane będą z odrębnych, nie objętych certyfikacją wzmacniaczy mocy, jakie połączone będą równolegle do CDSO z systemem komentatora sportowego.

Jak łatwo się domyślić zastosowanie pojedynczego systemu dźwiękowego, który łączyć będzie w sobie funkcje nagłośnienia sportowego oraz dźwiękowego systemu ostrzegawczego przynosi wiele korzyści. Mowa tu przede wszystkim o redukcji kosztów sprzętu, okablowania i nakładów pracy niezbędnych do instalacji. Istotnym plusem jest też ograniczenie liczby urządzeń nagłaśniających w obiekcie, ponieważ w ten sposób unika się montażu w jednej przestrzeni dwóch grup urządzeń. Kryterium zastosowania tego rozwiązania w praktyce będzie wielkość obiektu, ponieważ należy pamiętać, że w przypadku DSO system posiadać musi własne zasilanie rezerwowe w formie baterii akumulatorów, co w przypadku obiektów wymagających więcej niż kilku kW nagłośnienia może przekreślać sens ekonomiczny przedsięwzięcia. ■

mgr inż. Krzysztof Młudzik
Czynny elektroakustyk z wieloletnim doświadczeniem w branży systemów bezpieczeństwa. Ukończył studia na Katedrze Systemów Multimedialnych Politechniki Gdańskiej. Pracował m.in. w firmach TOA Electronics oraz Ambient System, w której pełni aktualnie funkcję dyrektora technicznego.



INTELIGENTNA WTYCZKA – AUTOMATYKA BUDYNKOWA W SYSTEMIE ALARMOWYM

Systemy sygnalizacji włamania i napadu coraz częściej zaliczają się do podstawowego wyposażenia obiektów mieszkalnych, biurowych itp. I choć mają przede wszystkim skutecznie wykrywać oraz sygnalizować wystąpienie ewentualnych zagrożeń, to część z nich oferuje „ponadstandardowe" funkcje stanowiąc ciekawą alternatywę dla instalacji smarthome.

Realizacja funkcji automatyki w ramach systemu alarmowego jest możliwa, nawet jeśli w obiekcie nie zostało przygotowane okablowanie uwzględniające montaż modułów sterujących. Można bowiem sięgnąć po urządzenia bezprzewodowe, takie jak inteligentne wtyczki ASW-200. Urządzenia te są częścią dwukierunkowego systemu bezprzewodowego ABAX 2, którego kontrolery (modele ACU-220 i ACU-280) współpracują z centralami alarmowymi SATEL z rodzin INTEGRA, INTEGRA Plus oraz VERSA. Warto dodać, że moduł ACU-220 znajdzie zastosowanie także w instalacjach bazujących na innych, dowolnych centralach alarmowych lub sterownikach automatyki.

Inteligentna wtyczka

Bezprzewodowy sterownik ASW-200 ma postać niewielkiej wtyczki i dostępny jest w dwóch wariantach: ASW-200 E do gniazd typu E (EURO – z bolcem ochronnym) oraz ASW-200 F do gniazd F (SCHUKO). Instalacja jest wyjątkowo prosta – ASW-200 wkłada się wprost do gniazda wtykowego instalacji 230 V AC, zaś do niej podłącza się odbiornik. Niewielkie wymiary sprawiają, że gdy sterownik jest podłączony do listwy zasilającej, nie blokuje sąsiadujących gniazd, co mogłoby mieć miejsce w przypadku większych konstrukcji.

ASW-200 może służyć do sterowania szerokim wachlarzem urządzeń elektrycznych o mocy nieprzekraczającej 2300 W – mogą być to m.in. lampy, wentylatory oraz różnego rodzaju sprzęt AGD czy RTV. Wyposażony jest w szereg mechanizmów zapewniających bezpieczeństwo pracy, w tym zabezpieczenia przed przeciążeniem oraz przed przegrzaniem. Jego estetyczna, kompaktowa obudowa wykonana jest ze specjalnego niepalnego tworzywa, co także ma niebagatelne znaczenie dla bezpieczeństwa.

Urządzenie wyposażone jest w podświetlaną przez diody obręcz z przezroczystego tworzywa, czyli tzw. LED Ring. Dostępne są dwa tryby jego pracy. Pierwszy to tryb monitorowania, w którym wskaźnik świeci na jeden z 32 kolorów, przy czym barwa jest zależna od prądu, który jest aktualnie pobierany przez podłączony do wtyczki odbiornik. Kolory zmieniają się płynnie przechodząc od niebieskiego, przy minimalnym poborze (lub jego braku), przez zielony przy obciążeniu ok. 300 W, aż do czerwonego przy maksymalnym poborze (ok. 2300 W). Dodatkowo LED Ring sygnalizuje m.in. rozruch, reakcje na komendy sterujące, a także awarie: miganiem na żółto informuje o przeciążeniu, zaś gdy błyska w kolorze czerwonym oznacza to, że przekroczona została dopuszczalna temperatura. Drugi tryb pracy, to ciągłe świecenie na jeden wybrany kolor. Funkcję świetlną można także wedle uznania zupełnie wyłączyć.

Sterowanie – ręcznie lub automatycznie

Użytkownik może, w zależności od potrzeb, włączać i wyłączać podłączone do ASW-200 urządzenia lokalnie, przyciskiem na obudowie wtyczki lub zdalnie, za pośrednictwem połączonego z centralą alarmową pilota, manipulatora lub z aplikacji służącej do sterowania systemem alarmowym. Wtyczka może być też włączana / wyłączana zgodnie ze scenariuszem zaprogramowanym w ramach systemu alarmowego i automatyki. Przykładowo, część oświetlenia w obiekcie może pracować w sposób zautomatyzowany, np. według ustalonych harmonogramów, bazując na informacjach z czujnika zmierzchu lub po wykryciu człowieka przez zamontowaną w danej lokalizacji czujkę ruchu. Aby ułatwić sobie życie, ASW-200 zastosować można przy urządzeniach, których podłączanie i odłączanie od zasilania może być nieco utrudnione. Mowa tu m.in. o routerach/modemach, kamerach czy oświetleniu choinkowym, czyli sprzęcie korzystającym najczęściej z gniazd mieszczących się w trudniej dostępnych miejscach. Wtyczka

sprawdzi się także przy codziennym włączania/wyłączania zasilaczy od laptopów czy ładowarek USB. Dla oszczędności energii ASW-200 może na czas nieobecności domowników, gdy system alarmowy czuwa, odłączać od zasilania zbędne urządzenia elektryczne, także te normalnie pozostające w trybie stand-by.

W przypadku central INTEGRA Plus skorzystać można z wyjść typu termostat – jeśli za pośrednictwem wtyczki podłączony zostanie klimatyzator lub grzejnik (oczywiście o mocy nieprzekraczającej dopuszczalnej), wtyczka może odpowiednio włączać i wyłączać te urządzenia, zgodnie z zaprogramowanymi progami temperatury odczytywanej przez współpracujące z centralą czujniki temperatury.

Inne urządzenia sterujące

Oprócz ASW-200, w ramach systemu ABAX 2 dostępne są też inne modele urządzeń, które znajdują zastosowanie przy realizacji funkcji automatyki budynkowej. Jednym z nich jest ASW-210, czyli dwukanałowy sterownik 230 V AC przeznaczony do montażu dopuszkowego. Wykorzystać można także komunikujące się drogą radiową z kontrolerem systemu ABAX 2 ekspandery urządzeń przewodowych. Moduły te posiadają po 4 programowalne wejścia i 4 wyjścia przewodowe. Moduł miniaturowy ma oznaczenie ACX-210 i posiada wyjścia typu OC, zaś większy model ACX-220 wyposażony jest w wyjścia przekaźnikowe. ■

Satel
MADE TO PROTECT

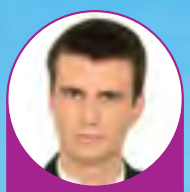
Artykuł Firmy **SATEL**

ZAPRASZAMY DO LEKTURY

Wersja online do pobrania na stronie:
www.ochrona-bezpieczenstwo.pl

ZASTOSOWANIE DRONÓW (BSP) W OCHRONIE OSÓB I MIENIA

Małgorzata Żmigrodzka



Marek Kustra

Ochrona osób i mienia jest jednym z obszarów, w których drony zdobywają coraz większe spektrum zastosowania. Przy wyposażeniu BSP w odpowiedni osprzęt jest on w stanie przesłać w czasie rzeczywistym właścicielowi nagranie, np. z włamania, a także powiadomić policję, jeżeli jest taka konieczność. Technologia bezzałogowa umożliwia również wykrywanie innych zagrożeń, takich jak: pożary czy powodzie. Nagrania oraz livestreamy przesyłane przez urządzenia łączności są źródłami precyzyjnych danych o niebezpieczeństwie i konieczności podjęcia stosownych działań.

Stale rośnie zainteresowanie wykorzystaniem dronów w służbie bezpieczeństwa publicznego, zwłaszcza przez osoby dokonujące działań w ramach pierwszorzutowej interwencji. Wysłanie człowieka – ratownika w rejon katastrof, pożaru, zawaliska związane jest ze znacznym ryzykiem, natomiast wysłanie specjalistycznego sprzętu celem przeprowadzenia rozpoznania bywa niemożliwe, stąd dobrym rozwiązaniem jest wykorzystanie drona. Warto zaznaczyć, że jesienią 2016 roku strażacy z Nowego Jorku rozpoczęli testy wartego 85 tys. USD drona wyposażonego w czułe kamery o wysokiej rozdzielczości (działające także w podczerwieni), który ma za zadanie znajdywać ludzi uwięzionych w pożarach[1].

Z zakresu ochrony mienia, BSP są właściwym narzędziem do prowadzenia monitoringu infrastruktury krytycznej państwa. Obserwacjom podlegają m.in.: rafinerie, stacje benzynowe, sieci energetyczne, linie wysokiego napięcia, elektrownie, jak i linie transportowe, np. kolejowe[2]. Jednym z przykładów jest PKP Cargo używające BSP do obserwacji transportowanych materiałów, przekazując obraz w czasie rzeczywistym zespołowi operacyjnemu. Rozwiązanie to jest niezwykle skuteczne, dzięki wykorzystaniu kamer

[1] Drony pomogą strażakom z Nowego Jorku, Chip, http://www.chip.pl/news/wydarzenia/tren-dy/2016/09/drony-pomoga-strazakom-z-nowego-jorku (12.09.2016)

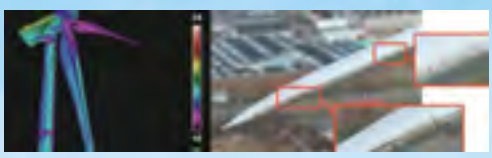
[2] J. Kozuba, E. Krakowiak, *Development of the civil use of unmanned aerial vehicles*, „Scientific Journal" No. 4/2016 (31), WSOSP, Dęblin 2016, s. 45.

o dużej jakości zbliżenia, dzięki którym dokładnie widać sylwetkę, rysy twarzy oraz inne znaki rozpoznawcze umożliwiające rozpoznanie ewentualnych złodziei. Rafinerie to kolejny przykład obiektów podlegających inspekcjom, które z powodzeniem są przeprowadzane przy zastosowaniu bezzałogowych aparatów latających. Inspekcjom stanu technicznego podlegają także mosty i wiadukty, których uszkodzenie mogłoby skutkować katastrofą w ruchu lądowym[3] (rysunek 1).

Rysunek 1. BSP podczas monitoringu transportu kolejowego oraz inspekcji mostów drogowych
Źródło: J. Kozuba, E. Krakowiak, Development of the civil use of unmanned aerial vehicles, „Scientific Journal" No. 4/2016 (31), WSOSP, Dęblin 2016, s. 45; S. Świerczyński, P. Zwolan, Wykorzystanie UAV w nawigacji, „Autobusy" 2019, nr 12, s. 212.

BSP posiadają również znaczny potencjał do stosowania w energetyce. R. Czapaj-Atłas oraz B. Dudek przeprowadzili badania, z których wynika, iż w zakresie energetyki BSP mogą służyć, np. do[4]:

- oceny stanu luster w fotowoltaicznych elektrowniach słonecznych;
- oceny stanu zniszczeń w elektrowniach atomowych;
- wykonania inspekcji turbin wiatrowych (rysunek 2) i hal elektrowni konwencjonalnych.
- inspekcji sieci elektroenergetycznych



Rysunek 2. Obraz uzyskany w wyniku inspekcji turbin wiatrowych z wykorzystaniem BSP
Źródło: S. Świerczyński, P. Zwolan, Wykorzystanie UAV w nawigacji, „Autobusy" 2019, nr 12, s. 211.

Bezzałogowe systemy powietrzne okazały się być również pomocne w działaniach prewencyjnych oraz przy zwalczaniu epidemii SARS-CoV-2. Z dużą skutecznością usprawniły pracę służb w zakresie weryfikacji przestrzegania kwarantanny, patrolowania miejsc publicznych i rozgłaszania komunikatów oraz poleceń służb przy pomocy głośników. Zastosowanie kamer termowizyjnych dało możliwość szybkiego wykrycia na rozległym obszarze osób z podwyższoną temperaturą. Dzięki temu możliwe stało się odseparowanie osoby potencjalnie zakażonej, zmniejszając w ten sposób ryzyko zakażenia innych ludzi. W zakresie zwalczania epidemii BSP stosowane były już także do dezynfekcji określonych obszarów poprzez zastosowanie podwieszanego zbiornika do oprysków ze środkiem dezynfekcyjnym.

Rysunek 3. BSP stosowane w epidemii SARS-CoV-2
Źródło: DJI, https://viewpoints.dji.com/blog/dji-helps-fight-coronavirus-with-drones, dostęp: 30.05.2022 r.

BSP są bardzo pożądane w branży nieruchomości, gdzie są wykorzystywane do fotografowania i filmowania budynków, które są oferowane przez dane przedsiębiorstwo, co pozwala na wizualizacje. Oczywiście drony mają szerokie zastosowanie także w branży budowlanej, gdzie wykorzystywane są do projektowania i wizualizacji terenów.

Innym zastosowaniem dronów mogą być badania termowizyjne istniejących obiektów budowlanych oraz bieżące kontrole stanu technicznego obiektów budowlanych. Przykładem jest zastosowanie platformy latającej do inspekcji budynku jednorodzinnego, co umożliwiło szybkie opracowanie dokładnej dokumentacji fotograficznej oraz filmowej dachu obiektu, który został uszkodzony wskutek silnego wiatru. Kolejny przypadek, dotyczył zastosowania drona w trakcie kontroli i opracowania dokumentacji zdjęciowej z niewielkiej odległości kluczowych elementów konstrukcji mostu, do których dostęp był znacznie ograniczony.[5]

Na uwagę zasługuje coraz częstsze zastosowanie dronów w rolnictwie. W USA i Australii coraz bardziej doceniane są zalety dronów, które znacznie oszczędzają czas i pieniądze rolników, służąc do monitoringu i ochrony mienia. Na ogromnych połaciach uprawianej roli można w szybki sposób bez wychodzenia z domu sprawdzić, w jakim stanie, np. wzrostu są dane uprawy

[3] S. Świerczyński, P. Zwolan, *Wykorzystanie UAV w nawigacji*, „Autobusy" 2019, nr 12, s. 211–212.

[4] R. Czapaj-Atłas, B. Dudek, *Drony, mini-i mikrodrony– przegląd obszarów zastosowań bezzałogowych statków powietrznych dla potrzeb monitoringu i inspekcji, w szczególności w obszarze energetyki*, „Energetyka", nr 8/2014, s. 485–492.

[5] Bezzałogowe statki powietrzne w kontroli obiektów budowlanych mgr inż. Tomasz Nowobilski Politechnika Wrocławska, Wydział Budownictwa Lądowego i Wodnego, Builder, 2020 r, s. 2.

na oddalonych gruntach. Takie drony mogą również fotografować i analizować przebieg wzrostu, ekspozycji na promienie słoneczne itp. Można również zawczasu wychwycić choroby, którymi zostanie zaatakowana uprawa, a rolnik może im zapobiec wcześniej, niż przy zwykłych metodach.

Rysunek 4. BSP w rolnictwie.
Źródło: http://www.swiatdronow.pl/drony-przyszloscia-rolnictwa, dostęp: 30.05.2022 r.

Powyższa analiza przykładowych metod zastosowania BSP na rzecz ochrony osób i mienia pozwala stwierdzić, że koncepcje użycia BSP zaczęły zastępować, czy wręcz wypierać dotychczasowe metody obserwacji, zbierania danych, czy innych zadań związanych pośrednio i bezpośrednio z bezpieczeństwem oraz ochroną. Jedną z głównych przyczyn jest fakt zmniejszenia ryzyka strat zasobów ludzkich oraz znacznie droższych urządzeń konwencjonalnych. BSP dają także możliwość prowadzenia niemal ciągłej obserwacji jak również zwiększają zakres monitorowanego obszaru w danej jednostce czasu w porównaniu do tradycyjnie rozumianych metod monitoringu i ochrony.

Bibliografia:
1. Bezzałogowe statki powietrzne w kontroli obiektów budowlanych mgr inż. Tomasz Nowobilski Politechnika Wrocławska, Wydział Budownictwa Lądowego i Wodnego, Builder, 2020 r, s.2.
2. Czapaj-Atłas R., Dudek B., *Drony, mini-i mikrodrony–przegląd obszarów zastosowań bezzałogowych statków powietrznych dla potrzeb monitoringu i inspekcji, w szczególności w obszarze energetyki*, „Energetyka", nr 8/2014
3. Kozuba J., Krakowiak E., *Development of the civil use of unmanned aerial vehicles*, „Scientific Journal" No. 4/2016 (31), WSOSP, Dęblin 2016
4. Szpakowski P., *Drony w walce z pandemią koronawirusa (SARS-CoV-2)*, „Safe Sky" nr 2(10)/2020, Polska Agencja Żeglugi Powietrznej
5. Świerczyński S., Zwolan P., *Wykorzystanie UAV w nawigacji*, „Autobusy" 2019, nr 12
6. http://www.chip.pl/news/wydarzenia/tren-dy/2016/09/drony-pomoga-strazakom-z-nowego-jorku

Dr Małgorzata Żmigrodzka
Lotnicza Akademia Wojskowa

Mgr inż. Marek Kustra
Lotnicza Akademia Wojskowa

SYSTEMY BEZPIECZEŃSTWA W GARAŻACH PODZIEMNYCH

W garażach podziemnych występuje szereg zagrożeń, a jednym z największych z nich jest możliwość wystąpienia pożaru. Wynika ona z obecności samochodów zasilanych łatwo palnym paliwem, w tym gazem LPG. Dlatego w większości garaży zamontowane zostały systemy detekcji, a także wentylacja bytowa i przeciwpożarowa. Obecnie takie zabezpieczenia są już właściwie standardem. W jaki jeszcze sposób właściciele garaży chronią swoich klientów?

Damian Żabicki

Minimalne wymogi odnośnie ochrony garaży znaleźć można w przepisach oraz wytycznych europejskich. Dotyczą one przede wszystkim systemów wentylacji pożarowej.

Zadaniem systemów wentylacji oddymiającej w garażach jest umożliwienie bezpiecznego i skutecznego prowadzenia działań ratowniczych, a także zabezpieczających przed zniszczeniem konstrukcji budynku. Istotne jest także zapobieganie wystąpienia zadymienia w przejściach ewakuacyjnych, w sytuacjach, gdy znajdują się w nich jeszcze ludzie.

Samoczynne urządzenia oddymiające

Przepisy dotyczące stosowania w garażach samoczynnych urządzeń oddymiających zawarte są w rozporządzeniu Ministra Infrastruktury. Regulacje, o których mowa, odnoszą się do garaży zamkniętych, o powierzchni całkowitej przekraczającej 1500 m2. W garażach otwartych nie ma obowiązku stosowania tego typu urządzeń – wystarczy naturalny przewiew każdej kondygnacji.

Zgodnie z literą prawa, sprawność wentylacji oddymiającej w garażu zamkniętym musi umożliwiać usuwanie dymu na takim poziomie, który pozwoli na to, aby podczas ewakuacji ludzi na chronionych przejściach i drogach ewakuacyjnych poziom zadymienia i temperatura pozwalały na bezpieczne opuszczenie garażu. Ewakuowanym ludziom musi także zostać zapewniony stały dopływ powietrza z zewnątrz, tak aby uzupełniał on deficyt powietrza usuwanego z pomieszczeń wraz z dymem. Rozporządzenie reguluje także parametry wentylatorów. Zgodnie z nim powinny mieć klasę F60060, gdy istnieje możliwość, że temperatura dymu przekroczy 400 stopni C, klasę F400120 w pozostałych przypadkach, ewentualnie inne klasy, zapewniające bezpieczeństwo ekip ratowniczych.

Tryskacze i zraszacze

W niektórych przypadkach w garażach zamkniętych należy dodatkowo zamontować urządzenia

do gaszenia – tzw. tryskacze lub zraszacze. Dotyczy to przede wszystkim garaży w obiektach z punktami gastronomicznymi obsługującymi powyżej 600 osób, lub w pomieszczeniach wysokościowych – użyteczności publicznej lub zamieszkania zbiorowego.

Jeśli w projekcie zakładane jest zastosowanie stałych urządzeń gaśniczych wodnych, możliwe jest powiększenie dopuszczalnej powierzchni strefy pożarowej garażu zamkniętego z 5 000 do 10 000 m^2. Co więcej, w takim przypadku jedna strefa pożarowa może obejmować więcej niż jedną kondygnację, a przejście ewakuacyjne może mieć długość nie 40 a 60 m.

Wentylatory kanałowe

W oddymieniu garażu skuteczna jest mechaniczna wentylacja oddymiająca kanałowa. Dzięki niej dym i ciepło utrzymane jest pod stropem, a powietrze na dole jest czyste, umożliwiając ewakuację i akcję gaśniczo-ratowniczą. To stosunkowo kosztowna izolacja, a do tego wymagająca odpowiedniej ilości miejsca pod stropem.

Jeśli chodzi o wentylatory wyciągowe, to powinny być uruchamiane bezpośrednio po wykryciu pożaru. Czasem stosuje się celowe opóźnienie, aby przeprowadzić sprawną ewakuację ludzi. Należy przy tym pamiętać, że takie opóźnienie grozi ewakuacją w warunkach większego zadymienia i wyższej temperatury. Dlatego do prawidłowego określenia czasu tego opóźnienia wykorzystywane są symulacje komputerowe CFD lub SHEVS (Smoke and Heat Exhaust Ventilation System).

Wentylacja strumieniowa

Do najskuteczniejszych systemów wentylacji mechanicznej należy wentylacja strumieniowa (impulsowa), stosowana jako alternatywa dla rozwiązań kanałowych. W standardowych warunkach wentylatory strumieniowe narzucają ukierunkowany przepływ powietrza w stronę wyciągu. W sytuacji, w której czujniki zarejestrują wzrost stężenia toksycznych gazów, system wentylacji strumieniowej rozpoczyna ukierunkowywanie przepływu zadymienia w sposób pozwalający na jego jak najszybsze usunięcie, oczywiście zapewniając jednocześnie ochronę dróg ewakuacyjnych. Działanie to opiera się na efekcie tłoka, a zanieczyszczenia są kierowane od nawiewu do otworu oddymiającego.

Wentylacja strumieniowa może być częścią systemu kontroli rozprzestrzeniania się dymu i ciepła lub systemu oczyszczania z dymu. W pierwszym przypadku dym i ciepło przetłaczane są w całym przekroju strefy, w kierunku od miejsca pożaru do punktów wyciągowych, ułatwiając działanie służb gaśniczych. Drugie rozwiązanie polega na rozcieńczaniu dymu, a jego wadą jest brak możliwości dostarczenia strażakom i osobom ewakuowanym czystej od dymu drogi do źródła ognia.

Decydując się na zastosowanie wentylacji strumieniowej, trzeba pochylić się nad prawidłowym rozmieszczeniem wentylatorów strumieniowych. Chodzi o to, aby w garażu nie występowały przestrzenie, które w czasie jego normalnej eksploatacji są niewentylowane. Co więcej, system oddymiania musi zapewnić skuteczność bez względu na to, w którym miejscu garażu pojawi się ogień. Sprecyzowana została także łączna wydajność uruchomionych wentylatorów strumieniowych. Nie może być ona większa od łącznej wydajności wentylatorów wyciągowych. Z kolei prędkość przepływu powietrza na przejściach ewakuacyjnych musi być mniejsza niż 5 m/s.

Jeśli chodzi o uzupełnianie powietrza, aby nie doszło do recyrkulacji dymu, powinno ono być dostarczane z prędkością mniejszą niż 2 m/s. W praktyce aby uzyskać te cele, garaż dzieli się na strefy detekcji dymu, które nie są większe niż 2000 m2. Strefy te wyposażone są w systemy sygnalizacji pożaru, z czujnikami dymu, ciepła lub z czujnikami multisensorowymi, które przesyłają do centrali systemu oddymiania informację o miejscu pojawienia się pożaru.

Wentylacja strumieniowa w garażach zamkniętych pełni jednocześnie funkcję wentylacji bytowej i oddymiającej. Intensywność wentylacji jest regulowana według intensywności ruchu i liczby samochodów, a także zgodnie z progami określonymi przez detektory CO, LPG i metanu. Uruchomienie wentylacji w wyniku przesłania przez detektory sygnału powinno nastąpić bez względu na tryb przewietrzania ze spalin. Zalecane są dwa progi intensywności usuwania gazów trujących i wybuchowych.

Rodzaje sensorów w systemach detekcji

Detektory gazów w garażach zamkniętych mogą reagować na obecność jednego konkretnego gazu, lub określać stężenie kilku różnych.

Na systemy detekcji przede wszystkim składają się czujniki. W garażach zwykle stosowane są czujniki półprzewodnikowe, czyli progowe, uruchamiające wentylację w sytuacji przekroczenia zadanych progów stężenia gazów. Czujniki tego typu są niezawodne i trwałe, ich wadą jest jednak to, że z czasem zwiększają swoją czułość, co wymaga ich okresowej kalibracji. Najczęściej jest ona przeprowadzana co 3 lata, a dla ułatwienia wzorcowania współczesne detektory posiadają wymienne moduły sensoryczne, w związku z czym tylko ten element w rzeczywistości podlega kalibracji.

Stosunkowo mniej popularnymi sensorami służącymi do wykrywania CO, są czujniki elektrochemiczne. Cechuje je dokładność i szybkość oraz brak konieczności przeprowadzania ponownej kalibracji. W garażach znaleźć można także sensory katalityczne oraz absorpcyjne IR, działające w oparciu o podczerwień.

Zasada działania systemów detekcji

Standardowo w garażach działa wentylacja bytowa. W sytuacji otrzymania sygnału o przekroczeniu progów alarmowych CO lub LPG, włączają się wentylatory wywiewne o odpowiedniej wydajności.

Działanie cyfrowych systemów detekcji gazów w garażach opiera się na mikroprocesorach, które sterują pomiarem stężenia, kompensacją termiczną, kalibracją bez ingerencji w wewnętrzne obudowy, odczytem historii zdarzeń i wymianą informacji z urządzeniami podłączonymi pod wyjścia (są to m.in. zewnętrzne sygnalizatory, sterownik układu wentylacji czy centralka). Najczęściej stosowanymi są detektory selektywne, a zatem oparte na sensorach elektromechanicznych lub działających na podczerwień.

Niezwykle istotne jest miejsce, w którym należy zamocować detektor. Tlenek węgla gromadzi się na początku w górnej części garażu, a po zmieszaniu z powietrzem wypełnia całą przestrzeń.

Natomiast LPG jako gaz jest cięższy od powietrza, co powoduje, że zbiera się na poziomie posadzki. W związku z tym czujniki wykrywające LPG należy montować jak najniżej.

Za prawidłową pracę wentylatorów w trybach bytowym oraz pożarowym odpowiada automatyka. To za jej pomocą regulowana jest szybkość działania wentylatorów, a także otwieranie klap. Automatyka działa w oparciu o sygnały z czujników CO i LPG oraz z systemu sygnalizacji pożaru i najczęściej tworzona jest indywidualnie pod dany system wentylacji.

Niezależnie od przyjętego rozwiązania, tylko regularnie przeprowadzane czynności serwisowe systemów detekcji CO i LPG gwarantują bezpieczeństwo i komfort użytkowania garaży i parkingów podziemnych. Działanie systemów detekcji CO i LPG należy kontrolować minimum raz w roku.

Podsumowanie

Wspomniane symulacje komputerowe dały odpowiedzi na szereg pytań związanych z wyposażeniem garaży w sprawne systemy bezpieczeństwa. Bez wątpienia, instalacje tego typu powinny być uruchamiane samoczynnie po wykryciu obecności gazu – zresztą, obligują do tego przepisy. Istotne jest, aby detektory umieszczane były w miejscach gromadzenia się gazu, a systemy wentylacji w garażu zapewniały wystarczający przepływ powietrza w obszarze znajdującym się przy posadzce. Dzięki temu gaz zostanie poderwany i odprowadzony z pomieszczeń.

Na zakończenie warto dodać, że w niektórych garażach podziemnych stosowany jest zakaz wjazdu pojazdów zasilanych LPG, co ma zapobiegać gromadzeniu się tego gazu. Niedawno rozgorzały dyskusje nad wprowadzeniem podobnego zakazu w przypadku samochodów elektrycznych, które trudno jest ugasić. Jeśli jednak elektryki mają być przyszłością motoryzacji, konieczne będzie znalezienie sposobu na zapewnienie bezpieczeństwa bez wykluczania ich obecności w garażach. Bo jeśli zakazy wjazdu samochodów poszczególnych kategorii będą się mnożyć, wkrótce może się okazać, że garaże przestaną pełnić swoją funkcję i staną się zbędne. ■

Damian Żabicki
Dziennikarz, analityk specjalizujący się w tematyce technicznej i przemysłowej

ANATOMIA ATAKÓW CYBERNETYCZNYCH

Grzegorz Data

Atak cybernetyczny to wszelkiego rodzaju ofensywny manewr wykorzystywany przez państwa narodowe, jednostki, grupy, społeczeństwo lub organizacje, które atakują komputerowe systemy informacyjne, infrastrukturę, sieci komputerowe i/lub urządzenia komputerowe za pomocą różnych metod złośliwego działania, zwykle pochodzących z anonimowego źródła, które kradną, zmieniają lub niszczą określony cel poprzez włamanie się do systemu podatnego[1].

Z atakami typu zero–day mamy do czynienia, gdy informacja o błędach w oprogramowaniu nie jest publikowana, gdyż jej odkrywca sprzedaje ją cyberprzestępcom, a producent dowiaduje się o niej dopiero wtedy, gdy jest ona od pewnego czasu wykorzystywana do ataków. Niestety antywirusy głównie bazujące na różnorakich sygnaturach blokują złośliwy kod jedynie wtedy, gdy jest podobny do innego już znanego.

Historia

Za pierwszy „atak hackerski" tygodnik New Science uznaje przejęcie pasma radiowego przez brytyjskiego magika Nevila Maskelynego, podczas pokazu telegrafu radiowego Gugliemo Marconiego w sali The Royal Institution w roku 1903. Marconi chciał zaprezentować swój wynalazek przesyłający bezpieczne i bezprzewodowo wiadomości na długie dystanse. W tym celu ustawił swoje urządzenie nadające w Kornwalii, zaś odbiornik zainstalowano w londyńskim teatrze około 480 km dalej. Zgromadzona publiczność z niecierpliwieniem oczekiwała na pokaz. Jednak przed rozpoczęciem transmisji brytyjski fizyk John Fleming – współpracownik Marconiego zauważył, że odbiornik zarejestrował pewne wiadomości przesłane alfabetem Morse'a: „szczury, szczury, szczury". Później kilka wersów z Szekspira i parę obelg skierowanych przeciw Marconiemu. Maskelyne chciał udowodnić, iż przesyłanie informacji telegrafem nie jest bezpieczne, można przejąć informację i nadać zmodyfikowaną[2].

Pierwszym opisanym kinetycznym efektem działania (cyberatak kinetyczny to atak powodujący rzeczywiste fizyczne zniszczenia w infrastrukturze lub narażający życie ludzi) komputerowego konia trojańskiego była potężna eksplozja w ZSRR gazociągu transsyberyjskiego. Za eksplozję odpowiedzialne miało być CIA, które do przeprowadzenia sabotażu użyło zmodyfikowanego

[1] Scott D. Applegate, 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON 2012), [in:], ed by. C. Czosseck, R. Ottis, and K. Ziolkowski, NATO CCD COE Publications, Tallin 2012, pp. 195–208, www.ccdcoe.org.

[2] Marks, P., 2011. "Dot-dash-diss: The gentleman hacker's 1903 lulz". New Scientist, 24 12, https://www.newscientist.co

oprogramowania komputerowego. Stojący na czele Departamentu Sił Powietrznych w administracji Ronalda Reagana Thomas Reed w swoich wspomnieniach – w książce „*At the Abyss: An Insider's History of the Cold War*" opisał akcję, którą, jak twierdził, przeprowadziła CIA[3]. Na podstawie informacji przekazanych przez Władimira Wetrowa, pracownika I Zarządu Głównego KGB, francuskiemu wywiadowi, CIA ustaliła, że Sowieci chcą wykraść oprogramowanie niezbędne do obsługi gazociągu z jednej z kanadyjskich firm. Amerykańscy agenci skłonili więc firmę, która znalazła się na celowniku KGB, do przygotowania zmodyfikowanej wersji oprogramowania, zawierającej tak zwaną logiczną bombę, czyli lukę w kodzie, dzięki której pozornie poprawnie działający program, po określonym czasie miał doprowadzić do katastrofy. Z książki Reeda wynika, że plan udało się w pełni zrealizować. Sowieci wykradli wadliwe oprogramowanie, które następnie zostało użyte do obsługi turbin, zaworów bezpieczeństwa oraz pomp w gazociągu. W momencie uaktywnienia się logicznej bomby oprogramowanie ustawiło pompy, turbiny i zawory tak aby ciśnienie gazu przekroczyło dopuszczalne parametry łączeń i spawów, co doprowadziło do gwałtownego wzrostu ciśnienia, którego efektem była potężna eksplozja. Zarejestrowały ją nawet amerykańskie satelity, a Dowództwo Obrony Północnoamerykańskiej Przestrzeni Powietrznej i Kosmicznej początkowo było przekonane, że w rejonie gazociągu doszło do zdetonowania bomby atomowej, jednakże nie zanotowano impulsu elektromagnetycznego, który by świadczył o wybuchu nuklearnym. Nie było ofiar w ludziach, gdyż gazociąg przebiegał przez niezamieszkaną część Syberii, ale straty spowodowane całą akcją uderzyły w radziecką gospodarkę, dla której bardzo ważne były dewizy uzyskiwane ze sprzedaży gazu do Europy Zachodniej. Po ujawnieniu w 2004 roku przez Reeda szczegółów operacji pojawiły się wątpliwości, czy faktycznie miała ona miejsce. Rosyjskie media dotarły między innymi do oficera KGB w stanie spoczynku, który twierdził, że w 1982 roku faktycznie doszło do eksplozji gazociągu na Syberii, ale z powodu błędów konstrukcyjnych[4].

Drugiego października 1988 r. Robert Morris student Uniwersytetu w Cornell stworzył program składający się z 99 linii, który miał, w założeniu autora „zmierzyć rozmiar Internetu". Wykorzystywał on 3 luki w oprogramowaniu, hasła dostępowe do serwerów łamał metodą siłową dysponując słownikiem składającym się jedynie z 400 słów. Po pomyślnym wniknięciu do systemu robak m.in. sprawdzał czy jego kopia jest już uruchomiona w systemie, losowo (algorytm rzutu kostką) wybierał, która z nich ma pozostać w systemie, a która miała ulec samozniszczeniu. Jedna na siedem kopii Morrisa rezygnowała z „rzucania kostką" i działała dalej, niezależnie od innych obecnych wersji. Nie wiadomo, czy był to błąd w kodzie, czy próba zwiększenia szans na przeżycie robaka w systemie, jednak właśnie takie działanie prowadziło do „zatkania" zainfekowanej maszyny, co jest wczesnym atakiem DoS – na wielu komputerach jednocześnie działy dziesiątki kopii Morrisa. W efekcie zainfekowane zostało 6000 komputerów, czyli 10 % z wszystkich podłączonych wówczas do Internetu. Straty szacowano na kwotę pomiędzy 100 tysięcy a 10 milionów dolarów, autor po przyznaniu się do winy został skazany na 3 lata w zawieszeniu, 10 000 dolarów grzywny oraz 400 godzin prac społecznych. Morris obecnie jest profesorem MIT.[5]

Pierwszy publiczny i motywowany politycznie atak DoS przeprowadzono już 1994 roku, gdy grupa określająca się jako Zippies postanowiła zaprotestować 5 listopada (na ten dzień przypada angielskie święto zwane dniem Guya Fawkesa) przeciwko nowemu prawu zakazującemu organizacji imprez z mocną muzyką elektroniczną. Zaatakowane rządowe witryny zostały wyłączona na niemal tydzień. Nikt wówczas nie wiedział, w jaki sposób obronić się przed nowym zagrożeniem[6].

Cyber Kill Chain

Dla lepszego zrozumienia ataku cybernetycznego na organizację firma Lockheed Martin wprowadziła pojęcie „Cyber Kill Chain" przez analogię do używanej już w wojsku koncepcji ataku „F2T2EA" – Find, Fix, Track, Target, Engage, Assess (odnajdź, ustal, śledź, celuj, wykonaj, oceń). Proces ten określa, iż atak cybernetyczny składa się z 7 faz i tym samym organizacje mogą i powinny mieć kolejne możliwości wykrycia i powstrzymania ataku na każdym etapie. Etapy ataku ukazuje poniższy rysunek.

Poszczególne fazy ataku to:

Fazy przed atakiem

1. **Rozpoznanie** – badania, identyfikacja i wybór celu, często obejmujące indeksowanie stron internetowych, takich jak materiały konferencyjne oraz listy adresów e–mail, sie-

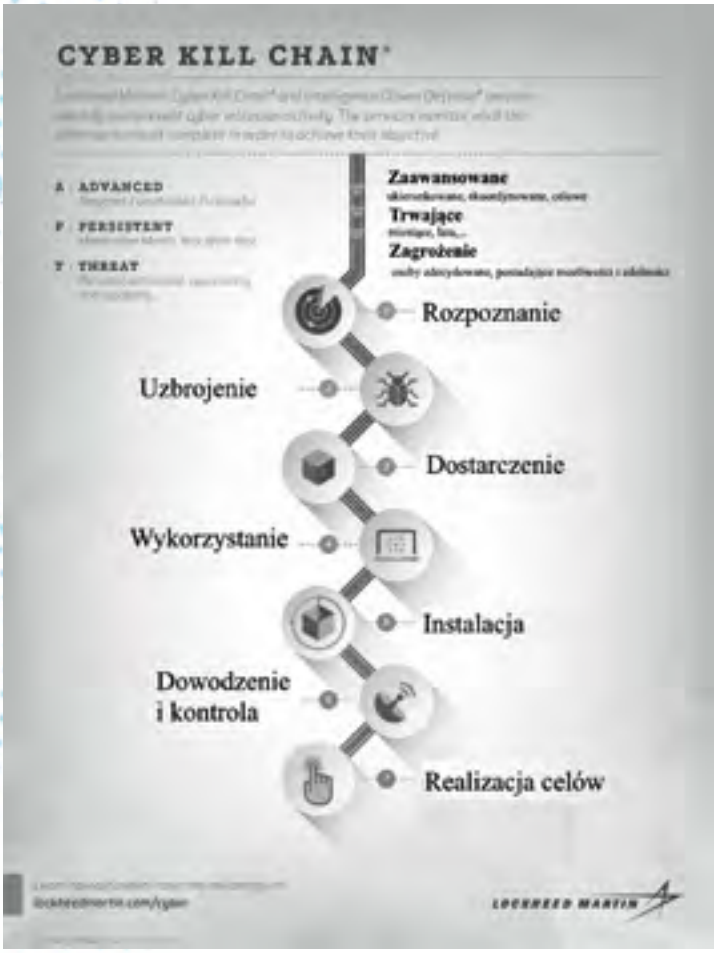
[3] T. Reed, At the Abyss: An Insider's History of the Cold War, Presidio Press 2005, Presidio P,

[4] The New York Times, William Safire, 2004. "The Farewall Dosier". http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html?_r=1

[5] Kaspersky, Lab, 2013. Kaspersky Daily blog: https://plblog.kaspersky.com/robak-morris-konczy-25-lat/669/

[6] Świechowski G. „Hacktywizm, czyli bunt internautów" http://www.pcworld.pl/news/Hacktywizm-czyli-bunt-internautow,368875.html

[7] E.M. Hutchins, M.J. Cloppert, and R.M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation 2011.



Rysunek 1. Fazy ataku cybernetycznego
Źródło: opracowanie własne na podstawie Hutchins, et al., 2011[7]

ci zależności oraz informacje na temat specyficznych technologii, atakujący nie musi nawet dotknąć sieci organizacji, wszystkie dane może pobrać przez wywiad z dostępnych z sieci źródeł;

2. **Uzbrojenie** – łączenie koni trojańskich (RAT – Remote Access Trojan) ze złośliwymi programami (ang. exploit) w celu stworzenia możliwej do dostarczenia paczki, często za pomocą automatycznego narzędzia (ang. weaponizer). Często jest to plik pdf, doc, skrypt, który potem zostanie umieszczony na uczęszczanej przez ofiarę witrynie.
3. **Dostarczenie** – przekazywanie ładunku do atakowanego środowiska. Najbardziej rozpowszechnione wektory dostawy dla „cyberbroni" w ramach ataków APT to załączniki e–mail (phising, spear–phishing), witryny internetowe (watering hole) i pendrive.

Fazy w trakcie ataku

4. **Wykorzystanie** – po dostarczeniu niebezpiecznego ładunku do środowiska ofiary jest uruchamiany złośliwy kod (najczęściej ofiara klika na link w mailu, instaluje „dodatkowy driver" by obejrzeć materiał video). Najczęściej wykorzystuje się luki w aplikacjach lub systemie operacyjnym. Ostatnio faza ta składa się z dwóch części uruchamiania, jest najpierw mały program trudny do zidentyfikowania przez antywirusy tzw. Downloader, który to następnie pobiera z sieci właściwy złośliwy kod.
5. **Instalacja** – instalacja konia trojańskiego (RAT – Remote Access Trojan) lub tylnych furtek (ang. backdoor) w systemie ofiary pozwala atakującemu na trwałe utrzymanie dostępu do środowiska organizacji.

Fazy po ataku

6. **Dowodzenie i kontrola** (ang. *Command and Control* – C2) – zaatakowany system wysyła sygnał do serwera kontrolnego o działaniu malware w celu ustanowienia kanału C2. Kierowanie aplikacją odbywa się ręcznie bądź automatycznie. Po ustanowieniu kanału C2 intruzi otrzymują pełny dostęp do zainfekowanego systemu. Do komunikacji używane są porty zwykle nieblokowane przez firewalle: http/https, ftp, dns, ostatnio także wykorzystywane są do sterowania komunikaty przekazywane przez sieci społecznościowe (Twitter, Facebook).
6. **Realizacja celów** – po przejściu przez pierwsze sześć faz intruzi mogą podjąć działania w celu osiągnięcia zamierzonych celów. Najczęściej jest to wykradzenie danych lub użycie systemu jako stacji przesiadkowej do przesłania emaila lub dojścia do innej sieci lub systemu (Hutchins, et al., 2011).

W celu maksymalizacji wykrycia zagrożeń, konieczne jest aby wszystkie fazy ataku były monitorowane. Matryca możliwych działań, które można podjąć na każdym etapie ataku przedstawiona jest w tabeli 1.

SecureWorks podaje kilka wytycznych do przerwania łańcucha ataku, proponując kwestie, które pomogą zrealizować system ochrony i przeciwdziałania atakom.

- **Poznanie przeciwnika** – Konieczne jest wdrożenie procesu rozpoznania zagrożeń celem ustalenia praktycznych informacji o samym zagrożeniu, aktorach (przeciwnikach) oraz ich działaniach. Konieczna jest pełna wiedza o własnych zasobach, systemach i sieciach.
  - Kim jest atakujący i jak działa,
  - Jakie ma taktyki, techniki i procedury,
  - Jakie posiada doświadczenie,
  - Jakie są wskaźniki jego ataku i którą fazę już osiągnął,
  - Czy jesteśmy gotowi przyjąć atak.
- **Wczesne rozpoznanie ataku** – Niezbędne jest elastyczne dostosowywanie polityk bezpieczeństwa i korelowanie informacji z różnych źródeł w celu osiągnięcia pełnego obrazu sytuacji.

Tabela 1. Sposoby postępowania z atakami.

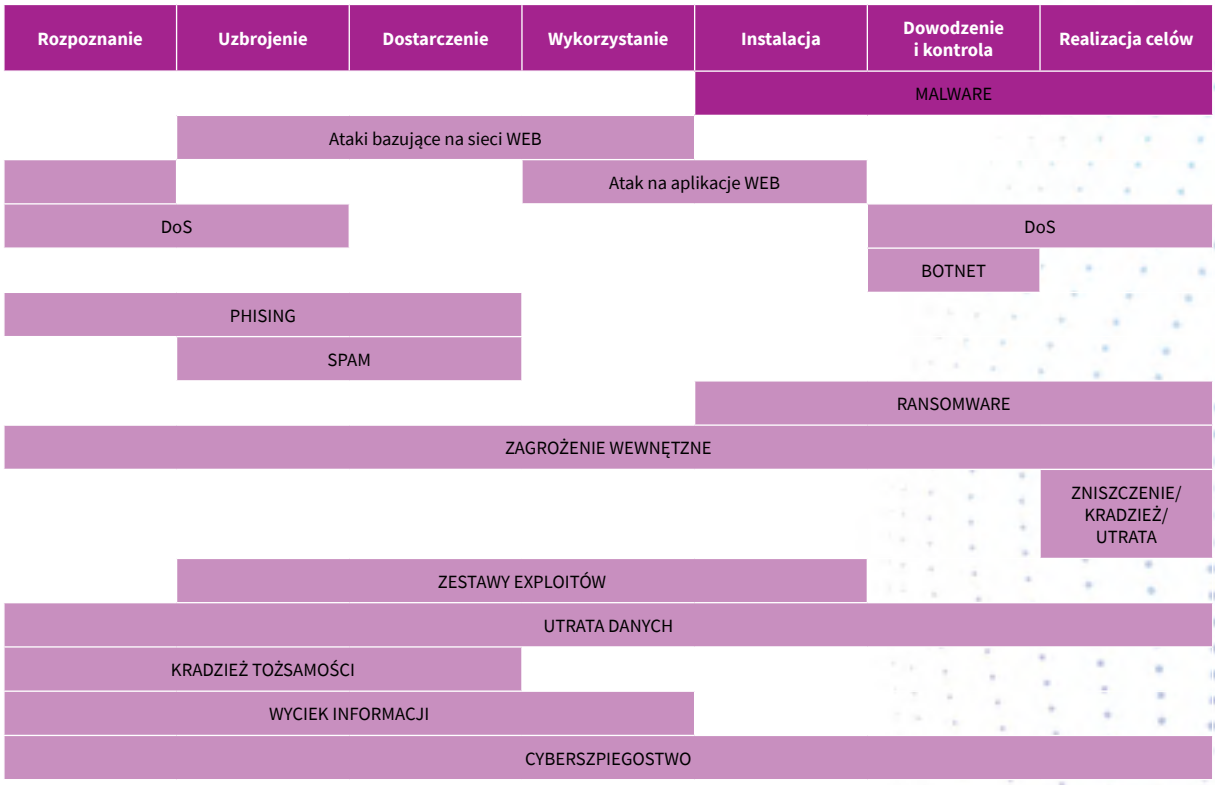
Faza	Detekcja	Blokada	Zakłócenie	Pogorszenie	Oszukanie
Rozpoznanie	Analityka witryny	Firewall			
Uzbrojenie	NIDS	NIPS			
Dostarczenie	Czujny Użytkownik	Filtr proxy	Antywirus	Kolejkowanie	
Wykorzystanie	HIDS	Aktualizacja	DEP		
Instalacja	HIDS	Środowisko chroot	Antywirus		
Dowodzenie i kontrola	NIDS	Firewall	NIPS	Serwer opóźniający (tarpit)	Przekierowanie DNS
Realizacja celów	Audyt logów			QoS	Honeypot

Źródło: (Hutchins, et al., 2011)

- Czy atakujący już funkcjonuje w sieci?
- Czy posiadamy narzędzia do wykrycia ataku?
- Czy potrafimy rozpoznać wszelkie wystąpienia ataku?
- Czy potrafimy stwierdzić wskaźniki wszystkich dotychczasowych faz ataku?
- Jak najszybciej potrafimy stwierdzić co jest celem ataku?

- **Zakłócenie ataku** – szefostwo musi ocenić realne szanse powodzenia operacji odparcia ataku a także umiejętności personelu. Jeśli odparcie jest niemożliwe bądź kwalifikacje załogi nie są wystarczające, konieczna będzie modyfikacja strategii dzięki informacjom zdobytym poprzez monitorowanie zagrożenia w czasie rzeczywistym.
  - Czy posiadamy narzędzia do wykrycia i zablokowania ataku?
  - Czy możemy ograniczyć rozprzestrzenianie się ataku?
  - Czy potrafimy przewidywać dalsze ruchy przeciwnika?
  - Czy wiemy dostatecznie dużo aby przyjąć atak przeciwnika?
  - Jak szybko możemy reagować?
- **Zwalczenie i usunięcie zagrożenia** – nie ma jednego panaceum na odparcie ataków,

Tabela 2. Ataki cybernetyczne rozłożone na poszczególne fazy



Źródło: autor na podstawie (ENISA, 2014).

Rysunek 2. ATTACK LIFE CYCLE
Źródło: Law Enforcement Cyber Center[8]

Cykl ten składa się z następujących faz:

- **rekonesans** – osint, infrastruktura sieciowa, informacje o kluczowych osobach, maile, profile społecznościowe, zakupy, przetargi, ogłoszenia, wersje os, przeglądarek, office, antywirusa firewall, wycieki,
- **początkowa kompromitacja** ((pierwsze przełamanie zabezpieczeń, otrzymanie danych logowania, watering hole, phising, spearphising (załączniki zip/rar /binarki/ pdf/office/skrypty/)),
- **ustanowienie przyczółku** – utrzymujemy się jak najdłużej chroniąc się przed wykryciem, instalacja backdorów (tygodnie, lata),
- **podniesienie uprawnień**,
- **wewnętrzny rekonesans** – serwery sieci, zasoby, architektura słabości, podatności, serwisy bazy danych,
- **ruchy boczne** (rozglądanie się),
- **utrzymanie obecności** (cicha reakcja łańcuchowa) – rozszerzenie obecności na innych maszynach zwykle aktualizują malware i instalują więcej zaawansowanych backdorów.

organizacje muszą oceniać swoją zdolność skutecznej reakcji na incydent. Specjaliści ds. bezpieczeństwa muszą oceniać i kontrolować przygotowanie organizacji do skutecznej reakcji na naruszenia bezpieczeństwa. Krytyczną kwestią jest posiadanie planu reakcji na wystąpienie incydentu informatycznego.

- Jakie systemy są zajęte przez atakującego?
- Jak odpowiedzieć na atak?
- Czy plan reakcji przewiduje ataki ukierunkowane?
- Czy potrafimy zapobiec kolejnemu atakowi?

Raport ENISA przedstawiony na rysunku 2 ukazuje typowe ataki rozłożone na poszczególne fazy kill-chain.

Attack Life Cycle firmy Madiant

Firma Madiant (obecnie zakupiona przez FireEye) badając atak chińskiej grupy hackerów (grupie nadano nazwę kodowa APT1 i udowodniono, iż jest to jednostka Chińskiej Armii Ludowo-Wyzwoleńczej nr 61398 zajmujących się włamaniami komputerowymi) opracowała swój model cyberataku nazwany Attack Life Cycle przedstawiony na rysunku 2.

ATT&CK

Organizacja MITRE rozszerzyła Cyber Kill Chain skupiając się na behawioralnych zachowaniach i technikach bazując na wieloletnim doświadczeniu i analizie ataków. Uznano, że o ile wiedza o początkowych etapach jest dobrze opisana, to należy skupić się na działaniach przeciwnika po otrzymaniu dostępu do systemów. Skrót (Adversarial Tactics, Techniques i Common Knowledge). Celem badaczy MITRE było rozbicie i klasyfikacja ataków w spójny i przejrzysty sposób, co ułatwi porównywanie i przeciwdziałanie im, aby dowiedzieć się, w jaki sposób atakujący wykorzystał badane sieci i punkty końcowe oraz przeniknął do nich.

ATT&CK bazuje na dużych macierzach, które opisują model działań przeciwnika, które przeciwnik może podjąć w celu złamania zabezpieczeń i pracy w sieci. Macierze pokrywają funkcjonowanie w systemach operacyjnych Linux, Windows oraz MacOS[9].

Model Diamentu

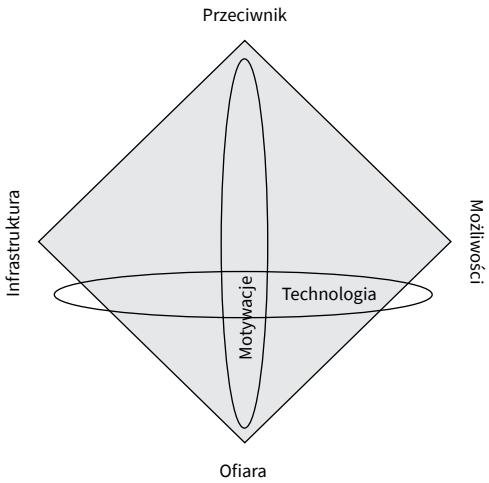
Inne podejście do oceny ataku informatycznego opublikowała organizacja Centre for Cyber Threat Intelligence and Therat Research w 2013 roku. Dokument ten skupia się na rozpoznaniu i zrozumieniu atakującego – jakich używa narzędzi, jaką posiada infrastrukturę, jakie ma motywacje. Zamiast analizować serie zdarzeń kładzie nacisk się powiązania pomiędzy cechami ataku. Nad poszukiwania źródeł pojedynczych ataków przekłada lepsze zrozumienie natury zagrożenia z którym mamy do czynienia. Model diamentu, przedstawiony na rysunku 14. pozwala na budowanie jaśniejszego obrazu działania przeciwnika pozwalające na sporządzenie bardziej efektywnej informacji o ataku. Dla przykładu modelowanie relacji na wiadomości phisingowej pozwala łatwiej ustalić kto wysłał, kto otrzymał maila, jakie adresy i domeny zostały użyte.

Korzyści stosowania modelu diamenu:

- umożliwia zastosowanie wskaźników kontekstowych i relacyjnych poprawiając współdzielenie rozpoznania o zagrożeniach cybernetycznych, poszerza zakres stosowania wskaźników,
- integruje pewność informacji z rozpoznaniem zagrożeń dzięki wykresom obrazującym atak,
- poprawia skuteczność analizy dzięki łatwiejszej identyfikacji pośrednich możliwości oraz prostszego budowania nowych analiz,

[8] CYBER ATTACK LIFECYCLE https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-life-cycle/

[9] MITRE, Adversarial Tactics, Techniques & Common Knowledge, https://attack.mitre.org/wiki/Main_Page



Przeciwnik	– adres email, telefon, zasoby sieciowe
Infrastruktura	– adres IP, nazwa domenowa, adres email
Możliwości	– malware, exploit, narzędzia hackerskie, skradzione certyfikaty
Ofiara	– osoby, zasoby sieciowe, adresy mail
Funkcje dodatkowe	– znacznik czasu, faza ataku, rezultat (sukces,porażka), kierunek

Rysunek 3. Model diamentu

- zwiększa dokładność analizy poprzez możliwość generowania hipotez, dokumentacji i badań poprzez większą dyscyplinę w procesie analitycznym,
- wspomaga prowadzenie rozwoju, planowania działań i strategii obrony poprzez łatwą integrację z większością platform,
- wzmacnia rozwój metod analitycznych poprzez sformalizowanie pierwotnych zasad na których można budować dalsze koncepcje,
- wspomaga opis zdarzeń w czasie rzeczywistym poprzez mapowanie procesu analitycznego do zrozumiałej klasyfikacji oraz detekcji włamań,
- określa podstawy aktywności, taksonomii, wymiany informacji o zagrożeniach oraz zarządzania wiedzą.

mjr Grzegorz Data
specjalista ds. informatyki i łączności
OISW w Rzeszowie

Reklama

KOMPLEKSOWE SYSTEMY BEZPIECZEŃSTWA W OPARCIU O IFTER EQU2

Główne zadania jakie stawiane są przed systemem bezpieczeństwa w Zakładach Karnych to:

- skuteczna kontrola nad przemieszczaniem się osób
- wykrywanie i identyfikacja osób opuszczających strefy bezpieczeństwa
- prosty i zrozumiały dla każdego funkcjonariusza system zarządzania
- wysoki poziom niezawodności z szybką diagnostyką uszkodzeń

Do realizacji tych zadań stosuje się System Kontroli Dostępu (SKD), Depozytory Kluczy (DK), System Sygnalizacji Włamania i Napadu (SSWiN), Ochronę Perymetryczną (OP), Telewizję Dozorową (CCTV), monitorowanie zasilania i torów transmisji danych. Żaden z tych systemów nie jest w stanie samodzielnie zapewnić pełnej ochrony obiektu, dlatego wymagana jest pełna i skuteczna koordynacja pracy tych systemów przez

system integrujący klasy IFTER EQU2. Zapewnia on oprócz integracji również pełną wizualizację w sposób prosty i czytelny przekazującą informacje o powstałym zagrożeniu. Mechanizmy prezentacji alarmów, powiadomień z przejścia przez śluzę i wiele innych, zostały dopracowane na wielu Zakładach Karnych pod potrzeby funkcjonariuszy. Jest to możliwe dzięki temu, że IFTER EQU2 jest produktem polskim i dla dobra klienta dbamy, aby mechanizmy opracowane dla jednego ZK pojawiły się już w standardzie dla pozostałych.

System Kontroli Dostępu

Głównym zadaniem tego systemu jest sprawne zarządzanie przemieszczaniem się funkcjonariuszy po Zakładzie Karnym oraz uniemożliwienie przemieszczania się osobom nieuprawnionym. Głównym zadaniem SKD jest sterowanie mechanizmem śluz (tylko jedne drzwi w danej chwili mogą być otwarte), sterowanie pracą krat z akceptacją w systemie nadzorczym i weryfikacją obrazu z kamer. Osoby oczekujące na otwarcie przejścia muszą być prezentowane na listach osób oczekujących z lokalizacją przejścia, ich danymi oraz zdjęciem. Jeżeli operator w zadanym czasie nie obsłużył danych drzwi, osoba musi być automatycznie usunięta z listy, łącznie z podglądem kamer na dane przejście. Na wizualizacji wymagana jest prezentacja aktualnego stanu drzwi, dynamiczne listy osób przemieszczających się przez przejścia oraz możliwość uproszczonego zarządzania SKD. Idealnie dla tych zadań sprawdza się najnowszy produkt firmy IFTER – EQU ACC G4 spełniający najwyższy czwarty poziom bezpieczeństwa według EN 60839-11-1. Na każdym etapie transmisja w tym systemie jest bardzo dobrze szyfrowana i zabezpieczona przed przepięciami. Posiada dodatkowo bogatą diagnostykę z rejestracją danych np. wartością napięcia 230VAC, zasilania akumulatora, kontrolera, czy nawet temperatury wewnętrznej kontrolera. Wejścia są parametryzowane, dzięki czemu mamy informacje z każdego wejścia o otwarciu, zamknięciu, sabotażu czy antymaskingu. Każdy kontroler w pamięci wewnętrznej przechowuje pełną konfigurację oraz dane 1mln kart i 0,5mln zdarzeń. Oprócz rozbudowanych możliwości konfiguracyjnych, administrator systemu może pisać własne skrypty rozbudowujące funkcjonalność w dowolnym zakresie.

Depozytor

Wymagane jest efektywne zarządzanie kluczami do pomieszczeń w połączeniu z SKD. Dodanie osoby do SKD umożliwia dodanie jej zezwolenia do pobierania kluczy. Usunięcie osoby z SKD automatycznie odbiera posiadane zezwolenia. Dodatkowo osoba, która nie zdała kluczy może nie zostać wypuszczona z ZK, a osoba, która nie została zarejestrowana na wejściu do ZK, nie będzie mogła pobrać kluczy.

System Sygnalizacji Włamania i Napadu

Do głównych cech systemów należy wykrywanie intruza. Do tego celu wykorzystuje się cały szereg czujników: otwarcia, ruchu, wibracji, zbicia szkła, bariery elektroniczne oraz przyciski napadowe, zorganizowanych w strefy alarmowe. Odczyt zdarzeń z centrali oraz sterowanie uzbrojeniem/rozbrojeniem stref alarmowych odbywa się przy pomocy klawiatur umieszczonych np. przy chronionym pomieszczeniu. W systemie bezpieczeństwa Zakładu Karnego, wykrycie intruza ma automatycznie pokazać obrazy z kamer z tego miejsca i prezentować go, aż do zakończenia incydentu. Na planach architektonicznych prezentuje się lokalizację alarmu oraz stan pozostałych systemów bezpieczeństwa.

Telewizja Dozorowa

Ze względu na dużą liczbę zamontowanych kamer na Zakładzie Karnym, operator nie jest w stanie obserwować wszystkich w sposób efektywny. Dlatego też prezentacja odbywa się jedynie w chwili wystąpienia jakiegoś zdarzenia i jest prowadzona do czasu jego zakończenia lub poprzez świadome wybranie przez operatora kamery na mapach wizualizacji w celu obserwacji danego obszaru. Wykrywanie zdarzeń najlepiej jest realizowane poprzez wykorzystanie rożnych zjawisk fizycznych (podczerwień, obwody magnetyczne, styki kontrolne), które po analizie w systemie włamaniowym czy kontroli dostępu powodują wywołanie obrazu z odpowiednich kamer. Oczywiście

w przypadku, gdy kamera ma wbudowaną obsługę protokołu Onvif-T może być wykorzystana jako element detekcyjny ruchu, którego centralką zarządzającą będzie system nadzorczy, co w połączeniu np. z ochroną obwodową i sumowaniu detekcji z czujników na ogrodzeniu i z kamery, może zmniejszyć ilość fałszywych alarmów. W tym zadaniu bardzo dobrze sprawdzają się rejestratory Digipryn francuskiej firmy Pryntec. Są to rejestratory klasy VMS, które można bardzo łatwo rozbudować o kolejne dyski oraz zarządzać wieloma rejestratorami przez wielu operatorów jednocześnie, korzystających z obserwacji obrazu on-line, archiwalnego oraz dokonujących analiz i raportów z wielu rejestratorów jednocześnie. Posiada elastyczną architekturę klient/serwer w pełni umożliwiającą zarządzanie użytkownikami i ich profilami, definiowanie centralnych zasad generowania raportów automatycznie rejestrowanych w systemie.

Funkcjonariusz nie łączy się indywidualnie do każdego rejestratora lecz ma w danej chwili dostęp do wszystkich kamer niezależnie od ich lokalizacji. Pozwala to na łatwe pobieranie i eksportowanie wideo, dokonywanie inteligentnego przeszukiwania archiwalnych zapisów, weryfikowanie stanu systemu (stan dysków, kamer, przekaźników, alarmy i zdarzenia). Dodatkowo umożliwia automatyczne monitorowanie (% dostępności i stan rejestratorów) oraz kompletną zdalną konfigurację sprzętu wraz z jego zdalną aktualizacją (rejestratorów, kamer …) oraz takich funkcji jak maski stref prywatności, czy też zarządzania zapotrzebowaniami na wideo (z możliwością definiowania daty, użytkownika, pliku, czasu trwania …). Dostępna jest również bardzo rozbudowana analityka obrazu pozwalająca automatycznie wykrywać zagrożenia, między innymi poprzez określanie ilości osób w danym obszarze, rozpoznawanie osób, pakunków itp.

Monitorowanie infrastruktury teletechnicznej

Do infrastruktury technicznej zaliczamy transfer danych oraz zasilanie. Większość urządzeń wykorzystuje do transmisji sieć komputerową. Monitorowanie dzięki temu ogranicza się do switcha po protokole SNMP, pozwalającym na weryfikacje czy podłączone urządzenie nie utraciło komunikacji, zmniejszyło lub zwiększyło transferu danych. Umożliwia również monitorowanie czy nikt nie podłączył do sieci nieautoryzowanych urządzeń oraz wiele innych parametrów pozwalających na szybkie wykrycie awarii lub przeciążeń. Monitorowanie zasilania realizowane jest zarówno przez monitorowanie poprzez SNMP pracy zasilaczy UPS, jak i analizatory sieci lub liczniki poprzez protokół Modbus IP lub Mbus. Pozwala to na rejestrację parametrów zasilania oraz wykrywanie przerw w zasilaniu. Monitorowanie infrastruktury technicznej umożliwia szybką diagnostykę awarii, oraz optymalizacji parametrów transmisji danych lub zasilania, minimalizując przerwy w transmisji danych lub zasilania.

Wizualizacja i integracja – IFTER EQU2

Wizualizacja IFTER EQU2 pozwala na pełną integrację i wizualizację wszystkich systemów bezpieczeństwa zainstalowanych na terenie Zakładu Karnego dodatkowo monitorując i diagnozując tory transmisji danych i zasilania.

Dzięki łatwej w obsłudze wizualizacji w oparciu o mapy architektoniczne nadzorowanych budynków, operator ma pokazaną dokładną lokalizację powstania incydentu z prezentacją obrazu on-line. Widząc rozmieszczone ikony kamer na planach i pobudzone czujniki lub otwarte drzwi, łatwo jest nadzorować przemieszczanie się intruza klikając na kolejne ikony kamer. Dodatkowo można do każdego czujnika skojarzyć kilka kamer, z których obraz będzie prezentowany automatycznie w chwili pobudzenia czujnika.

Pobudzanie kolejnych czujników powoduje podmianę najdłużej prezentowanego wideo na aktualnie obserwującego zagrożone miejsce.

Po zakończeniu incydentu, operator klikając na zdarzenie z czujnika włamaniowego lub drzwi automatycznie otwiera wideo z kamery obserwującej ten incydent. Pozwala to na minimalizację czasu niezbędnego do wykonywania weryfikacji. Dla zwiększenia efektywności przeglądania wideo na samym rejestratorze, IFTER EQU2 może wpisywać zdarzenia alarmowe lub np. odbicia kart z kontroli dostępu w znaczniki rejestrowanego obrazu. Wystarczy wtedy wpisać w rejestratorze np. Jan Kowalski, aby znaleźć sekwencje obrazu związane z tą osobą. Z drugiej strony wykryta i zidentyfikowana osoba przez kamery jest przekazywana do wizualizacji w celu określenia lokalizacji danej osoby lub pojazdu. Kontrola dostępu EQU ACC dzięki odczytanym tablicom rejestracyjnym pojazdów może sterować przejazdami pomijając zbliżenie karty do czytnika. Analogicznie dzięki identyfikacji osób EQU ACC może przydzielać dostęp do poszczególnych pomieszczeń. Alarmy i zdarzenia przesyłane z rejestratora Digipryn pozwalają na natychmiastowe wykrywanie problemów z utratą komunikacji z kamerą, które można dodatkowo zweryfikować w IFTER EQU2 kontrolując urządzenia odpowiedzialne za transmisję danych i zasilanie poprzez protokół SNMP (switch, router, UPS). Połączenie możliwości rejestratora Digipryn, EQU ACC i IFTER EQU2 pozwala na dostosowanie do oczekiwań bardzo wymagających klientów zarówno wojskowych jak i korporacyjnych o bardzo rozproszonej strukturze zarządzanych obiektów.

IFTER

Autor: Jerzy Taczalski

■ PROJEKT
BMS 2022

PROJEKT BMS.

Konferencja w obszarze zintegrowanych systemów automatyki budynkowej

23/24
listopada 2022

Centrum Konferencyjno-Wypoczynkowe
Pałac i Folwark Łochów

www.projektbms.pl

Reklama

BĄDŹ NA BIEŻĄCO Z WIEDZĄ FACHOWĄ!

PRENUMERATA 2023!

W CZASOPIŚMIE PUBLIKUJEMY TREŚCI DOTYCZĄCE:

- Monitoringu wizyjnego
- Kontroli dostępu
- SSWiN
- Ochrony perymetrycznej
- Termowizji
- Bezpieczeństwa pożarowego
- Ochrony infrastruktury krytycznej
- Systemów łączności
- Zasilania awaryjnego
- DSO

Prenumerata roczna:
69 zł

prenumerata@mediafachowe.pl 22 535 32 29 www.czasopisma.net

OCHRONA i BEZPIECZEŃSTWO OBIEKTÓW I BIZNESU
www.ochrona-bezpieczenstwo.pl

Czasopismo z branży ochrony pełni rolę doradczą, informacyjną, publicystyczną, propagującą wiedzę w obszarze ochrony i bezpieczeństwa obiektów oraz biznesu.

PRENUMERATA

Dział prenumeraty
Tel. + 48 22 53 53 229
prenumerata@mediafachowe.pl

Zamówienie prenumeraty przyjmujemy
- Telefonicznie **+ 48 22 53 53 229**
- e-mailem **prenumerata@mediafachowe.pl**
- przez internet **www.czasopisma.net**

Prenumerata
Roczna **69 zł**
Roczna studencka **50 zł**

Prenumerata dostępna także przez
- **RUCH S.A.**
- **Kolporter Sp. z o.o. S.K.A.**
- **Garmond Press S.A.**
- **G.L.M. Sp. z o.o.**
- **AS Press Andrzej Szlachciuk**

SKLEP INTERNETOWY
www.czasopisma.net

PRENUMERATA ELEKTRONICZNA DO POBRANIA NA STRONIE
www.ochrona-bezpieczenstwo.pl

Lubię to!

Wejdź na nasz profil i polub nas!

www.facebook.com/**ochronaibezpieczenstwo**

KONTAKT

Wydawca
Mediafachowe, ul. Wąski Jar 9
02-786 Warszawa, tel. +48 22 53 53 227

Prezes zarządu: **Katarzyna Polesińska**

Dyrektor wydawnicza
Joanna Jaworska
j.jaworska@euro-media.pl
tel. 606 911 070

Redakcja:
ul. Wąski Jar 9, 02-786 Warszawa
redakcja@ochrona-bezpieczenstwo.pl
www.ochrona-bezpieczenstwo.pl

Robert Gabrysiak
Redaktor prowadzący

redakcja@ochrona-bezpieczenstwo.pl
tel. 785 210 093

Lidia Tuchowska
Redaktor/Marketing i PR

tel. 604 995 466
l.tuchowska@ochrona-bezpieczenstwo.pl

Katarzyna Kalata-Kieblesz
Kierownik Działu Reklamy

tel. 604 588 851
k.kalata@ochrona-bezpieczenstwo.pl

Stała współpraca:
Jerzy Ciszewski, Urszula Garlińska, Mateusz Gosk, Sebastian Hładun, Dariusz Knapek, Waldemar Kubik, Marek Kustra, Krzysztof Łangowski, Paweł Łuszcz, Dobrosław Mąka, Cezary Mecwaldowski, Krzysztof Młudzik, Radosław Monia, Sergiusz Parszowski, Michał Pietrzak, Adam Radomyski, Robert Poklek, Janusz Sawicki, Stanisław Sulenta, Jerzy Taczalski, Norbert Tuśnio, Tomasz Sowa, Damian Żabicki, Małgorzata Żmigrodzka.

Zdjęcia: zespół redakcyjny, materiały promocyjne, www.stock.adobe.com/pl/

Łamanie i opracowanie graficzne: WAŻKA Łukasz Piotrowski

Prawa autorskie zastrzeżone. Przedruk i wykorzystywanie materiałów możliwe tylko po uzyskaniu pisemnej zgody Wydawcy. Redakcja nie ponosi odpowiedzialności za treść reklam, ogłoszeń oraz artykułów firmowych, ani za opinie wyrażone w artykułach, które pozostają prywatnymi Autorów.

ZAMEK ASP 03

Zamek nawierzchniowy jednostronnie otwierany
z zatrzaskiem (paniczny)

BEZPIECZEŃSTWO »

NIEZAWODNOŚĆ »

GWARANCJA JAKOŚCI »

Zamek ASP 03 nawierzchniowy jednostronnie otwierany przeznaczony do cel więziennych, krat przejściowych, furt więziennych, który znajduje zastosowanie w placówkach penitencjarnych. Posiada certyfikat IMP.

Mościska
ul. Chabrowa 32
05-080 Izabelin

tek: +48 22 722 86 90
fax.: +48 22 864 23 79
bank@klos.com.pl

› www.klos.com.pl ‹

KOMPLEKSOWE SYSTEMY ZABEZPIECZEŃ PRZECIWPOŻAROWYCH

- Systemy oddymiania
- Systemy napędów
- Systemy sygnalizacji pożarowej
- Systemy naturalnej wentylacji
- Systemy zamknięć ogniowych

www.dhpolska.pl

D+H
BUILDING ATMOSPHERE