CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 2(126)/2019

ZABEZPIECZENIA

Ulisse evo

Bądź świadkiem ewolucji wizyjnych systemów zabezpieczających

Kamera ULISE EVO PTZ firmy Videotec to kolejny, innowacyjny krok naprzód w dążeniu do tworzenia coraz skuteczniejszych i niezawodnych składników wizyjnych systemów dozorowych. Ta nowa, wszechstronna kamera PTZ jest konkurencyjna cenowo i ma niespotykany dotychczas wygląd.

VIDEOTEC

VIDEO SECURITY PRODUCTS
www.videotec.com
info@videotec.com
Made in Italy since 1986

deLux technology

ONVIF | S Q

RACS 5.5

System bezpieczeństwa, automatyki i kontroli dostępu

- Programowa integracja z centralami alarmowymi serii INTEGRA (SATEL)
- Tworzenie indywidualnych formatów eksportu danych RCP
- Wykonanie komendy globalnej w reakcji na wybrane zdarzenia
- Obsługa kamer CCTV BCS Line
- Monitorowanie strefy obecności w aplikacji webowej VISO WEB
- Udostępniono moduł wydruku kart w programie VISO ST
- Obsługa czytnika administratora HID OMNIKEY 5x27 CK

MCT86M-IO-CH-HR
Terminal dostępu do systemu RACS 5

Wysoka niezawodność i funkcjonalność potwierdzona
w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

roger®
Intelligence for Building

SPIS TREŚCI

Bezpieczniejsze parkingi
dzięki systemowi AXIS License Plate Verifier

Axis Communications wprowadza na rynek system automatycznej weryfikacji tablic rejestracyjnych **AXIS License Plate Verifier**, w który wyposażone są kamery. Produkt ten już zabezpiecza parkingi w wielu krajach europejskich.

Nowy produkt jest pierwszym opatentowanym systemem automatycznego rozpoznawania tablic rejestracyjnych (ang. *automatic license plate recognition* – ALPR) marki AXIS. Jest dostępny jako oddzielny system lub dostarczany w zestawie z VeriForce Kit AXIS P1445-LE-3. Axis Communications oferuje podsystemy do kontroli wjazdu i wyjazdu, w tym specjalne oprogramowanie oraz repozytorium scenariuszy. Rozwiązanie to sprawdzi się na zamkniętych parkingach, w strefach służących do magazynowania oraz obsługi środków transportu towarowego, w centrach logistycznych, w strefach dla pojazdów uprzywilejowanych. System jest otwarty, a więc daje możliwość rozbudowy w przyszłości.

W skład zestawu wchodzi kamera sieciowa AXIS P1445-LE i moduł analityczny AXIS License Plate Verifier z algorytmami ALPR. Kluczową funkcją systemu jest automatyczna obsługa wszystkich etapów weryfikacji dostępu (dla 1000 uprawnionych i 1000 nieuprawnionych pojazdów): rejestracji obrazu pojazdu, zarządzania listą pojazdów, decyzji dotyczących dostępu i sterowania barierami. Rozwiązanie to obejmuje również funkcję sterowania drzwiami, do którego niezbędny jest kontroler AXIS A1001 i oprogramowanie AXIS Entry Manager. Do zalet produktu należy duża liczba danych wejściowych (m.in. dzień tygodnia, pora dnia i godzina wjazdu lub wyjazdu), łatwa konfiguracja przez interfejs sieciowy, duża przepustowość, minimalne zaangażowanie personelu w aktualizację listy pojazdów i opcjonalne zapewnianie dostępu stronom trzecim (podwójne uwierzytelnianie, *anti-passback*, kontrola płatności).

Od 1 lutego 2019 roku asortyment jest dostępny za pośrednictwem kanałów dystrybucji firmy Axis Communications w Polsce, a także w pozostałych krajach Europy Środkowej i Europy Wschodniej.

Więcej szczegółowych informacji znajduje się na stronie https://www.axis.com/pl-pl/products/axis-license-plate-verifier.

Bezpośr. inf. Karol Dominiczak
Axis Communications

Sygnalizator SAW-6102
firmy POLON-ALFA

Nowy produkt firmy **POLON-ALFA** – **SAW-6102** – to konwencjonalny sygnalizator tonowy przeznaczony do pracy wewnątrz pomieszczeń. Współpracuje on ze wszystkimi centralami sygnalizacji pożarowej, które oferują na swoich wyjściach sygnalizacyjnych napięcie sterujące od 16 V do 32,5 V. Poziom natężenia dźwięku (w odległości do jednego metra) dochodzi do 114 dB. W odróżnieniu od SAW-6101 sygnalizator SAW-6102 charakteryzuje się mnogością trybów pracy. Pozwala na zsynchronizowanie sygnalizatorów działających w jednej przestrzeni akustycznej (dotyczy to zarówno sygnalizatorów SAW-6102, jak i SAW-6101). Nowy sygnalizator jest wyposażony w przycisk do wyciszania sygnału akustycznego.

SAW-6102 jest osadzany w gnieździe G-40S, do którego są przyłączane przewody zasilania oraz opcjonalne przewody do synchronizacji. Jego obudowa (IP 21C) jest wykonana z niepalnego czerwonego tworzywa. Urządzenie może pracować w temperaturach z zakresu od -21°C do +55°C.

Sygnalizator SAW-6102 jest wyposażony w przesuwny przełącznik składający się z ośmiu sekcji służących do wyboru tonu, głośności, sposobu zwiększania się głośności i synchronizacji. W zależności od potrzeb umożliwia to wybór jednego z 16 typów sygnału dźwiękowego, a cztery poziomy głośności dźwięku umożliwiają dostosowanie urządzenia do bardziej wymagających obiektów. Nowością zastosowaną w SAW-6102 jest opcja zwiększania się głośności sygnału dźwiękowego sygnalizatora.

Bezpośr. inf. POLON-ALFA

Kamery Bosch Flexidome IP starlight 8000i

Najwyższy poziom szczegółowości obrazu i bezpieczeństwa

Firma **Bosch** po raz kolejny wyznacza nowe standardy systemów telewizji dozorowej, wprowadzając do swojej oferty innowacyjne stałopozycyjne kamery kopułkowe **FLEXIDOME IP starlight 8000i**. Kamery są dostępne w rozdzielczościach od FullHD 1080p do 4K Ultra HD. W połączeniu z funkcjami Starlight i HDR zapewniają bardzo dobrą jakość i szczegółowość obrazu nawet w bardzo niekorzystnych warunkach oświetleniowych. Modele wytwarzające obraz z prędkością 60 kl./s znajdą zastosowanie w obserwacji scen o wysokiej dynamice ruchu.

Kamery mają nowoczesne funkcje do inteligentnego zarządzania strumieniem wizyjnym. Pozwalają one na znaczne zmniejszenie wymaganej przestrzeni dyskowej czy przepustowości sieci. Kamera jest standardowo wyposażona w funkcję analizy obrazu Intelligent Video Analytics, która automatycznie generuje alarm dla operatora i zwraca jego uwagę na miejsce, gdzie wystąpiło potencjalne zagrożenie. Te wszystkie rozwiązania zapewniają najwyższy poziom skuteczności systemu oraz umożliwiają interpretowanie odczytywanych informacji w celu podejmowania właściwych decyzji, również biznesowych, wykraczających poza sferę bezpieczeństwa.

Kamery Bosch serii Flexidome IP starlight 8000i wyróżniają się również cechami ułatwiającymi proces instalacji i uruchomienia systemu telewizji dozorowej. Ustawienie żądanego pola obserwacji na etapie konfiguracji odbywa się zdalnie dzięki funkcji regulacji położenia obiektywu. Oznacza to, że w trakcie montażu nie jest konieczne zdejmowanie kopułki i manipulowanie przy obiektywie. Dzięki temu możliwe jest zastosowanie innowacyjnej koncepcji szybkiej i pewnej instalacji w trzech prostych krokach. Wbudowany moduł służący do komunikacji bezprzewodowej daje możliwość konfiguracji kamery zaraz po jej zamocowaniu na miejscu użytkowania, z wykorzystaniem aplikacji na smartfonie lub tablecie. Wszystkie te zabiegi skracają czas potrzebny na montaż i uruchomienie kamery nawet o 75%.

Bezpośr. inf. Maciej Wróbel
Bosch Safety and Security Systems

Nowa seria czytników
marki KaDe

Oferta firmy **AAT HOLDING** została powiększona o nowe czytniki kart zbliżeniowych marki **KaDe – KDH-C130M, KDH-C130U, KDH-CK130M i KDH-CK130U** (dwa ostatnie to wersje z klawiaturą). Zastępują one czytniki serii KDH-C100 i KDH-C110, które zostały wycofane ze sprzedaży. Na uwagę zasługują modele z klawiaturą, których nie było w seriach 100 i 110. Przeznaczone są do systemów, których użytkownicy posługują się kartami zbliżeniowymi w standardzie Mifare albo Unique. Modele oznaczone literą *M* współpracują z kartami w standardzie Mifare (13.56 MHz, 34 bity), a czytniki oznaczone literą *U* – z kartami Unique (125 kHz, 26 bitów). Dzięki przełączanemu formatowi klawiatury (cztery albo osiem bitów jest wysyłane z czytnika po każdej wprowadzonej na klawiaturze cyfrze) możliwe jest zastosowanie czytników w systemach kontroli dostępu Kantech, KaDe oraz w innych, w których kontrolery obsługują interfejs wyjściowy Wiegand oraz różne formaty danych z klawiatury.

Nowe czytniki należą do tej samej, dobrze znanej, cieszącej się dużą popularnością i doskonale wkomponowującej się w każde wnętrze linii wzorniczej co modele serii KDH-C330-U/H/M i KDH-CK330-U/H/M. Czytniki są koloru czarnego. Ich ceny są bardzo atrakcyjne. Dzięki wytrzymałej obudowie z tworzywa sztucznego ABS oraz konstrukcji zapewniającej stopień ochrony IP66 czytniki KaDe serii 130 mogą być zastosowane zarówno wewnątrz, jak i na zewnątrz budynków.

Bezpośr. inf. AAT HOLDING

Sztuczna inteligencja
w systemach rozpoznawania tablic rejestracyjnych

Algorytmy automatycznego rozpoznawania tablic rejestracyjnych są już powszechnie wykorzystywane w systemach dozoru wizyjnego.

Dahua Technology posiada w swojej ofercie wiele kamer wykorzystujących ANPR (ang. *automatic number plate recognition*). Są one w stanie rozpoznać tablicę rejestracyjną, sprawdzić, czy odczytany numer jest w bazie danych, otworzyć bramę, a także wysłać powiadomienie operatorowi. Co więcej, do ich działania nie są już potrzebne drogie serwery.

Dahua Technology kilkukrotnie zajmowała pierwsze miejsce w mistrzostwach systemów OCR czy analizy treści obrazu (KITTI Vision Benchmark), a także ustanowiła nowy rekord świata w śledzeniu wielu obiektów jednocześnie (ang. *multiple object tracking*), na platformie do testowania algorytmów stworzonej przez Szwajcarski Federalny Instytut Technologii w Zurychu, Uniwersytet w Adelajdzie i Politechnikę w Darmstadt.

Dzięki tym doświadczeniom oraz najnowszym procesorom wykorzystującym sztuczną inteligencję inżynierowie z firmy Dahua Technology opracowali nową **kamerę LPR – ITC215-PW4I-IRLZF27135**.

Nowy procesor wykorzystujący sztuczną inteligencję zwiększył skuteczność rozpoznawania pojazdów i tablic o 300%. Nie tylko umożliwia on rozpoznawanie tablic, ale także jest w stanie określić kierunek poruszania się pojazdu i zakwalifikować go do jednego z jedenastu typów (samochód osobowy, bus, van, suv etc.). Urządzenie zostało wyposażone w najnowszy przetwornik Sony Full Color, który ma dwukrotnie większą czułość i szerszą dynamikę niż przetworniki STARVIS i STARLIGHT. Taka światłoczułość umożliwia pracę kamery w trybie kolorowym w dzień i w nocy, a także automatyczne rozpoznawanie kolorów pojazdów.

Kamera ma wejście CVI, które umożliwia podłączenie drugiej, pomocniczej kamery do kamery głównej. Możliwe jest wykorzystanie innej kamery panoramicznej. Takie połączenie nie tylko znacznie zwiększa skuteczność systemu, ale także redukuje koszty instalacji.

Dahua Technology po raz kolejny pokazuje, że wykorzystanie sztucznej inteligencji w wizyjnych systemach dozorowych to teraźniejszość, a tak zaawansowana kamera jak ITC215 może kosztować tyle, ile smartfon.

Bezpośr. inf. Mateusz Zapotoczny
Dahua Technology Poland

Farma serwerów AI

zredukowana do jednego urządzenia o wysokości 1U

Systemy rozpoznawania twarzy nie są nowym rozwiązaniem w branży VSS. Coraz częściej możemy usłyszeć o całych miastach i regionach, w których zainstalowano setki, a nawet tysiące kamer zintegrowanych z systemami rozpoznawania twarzy. **Dahua Technology** ma na swoim koncie kilka zrealizowanych projektów obejmujących całe prowincje, w których złapanie złodzieja zajmuje kilka minut dzięki nowoczesnym algorytmom. Niestety do tej pory wymagało to użycia wielu serwerów, przy czym każda jednostka miała wysokość 6U, a cały system pobierał tysiące watów i oczywiście kosztował dziesiątki tysięcy euro.

Nastąpił jednak przełom. Powstała seria urządzeń, dzięki którym osiągnięcie podobnych rezultatów jest możliwe z użyciem płyty głównej o wielkości tabletu, w systemie, który jest tak prosty w obsłudze jak tablet, a przede wszystkim w cenie tabletu!

Najnowsza seria rejestratorów Dahua z serii AI (Artificial Intelligence) oferuje zaawansowane algorytmy rozpoznawania twarzy i klasyfikacji obiektów. Urządzenia te mieszczą się w obudowach o wysokości 1U, a po podłączeniu praktycznie dowolnych kamer IP na żywo dokonują analizy treści obrazów w celu rozpoznania twarzy na maksymalnie czterech kanałach wizyjnych jednocześnie. Dostępna jest też wersja XVR dostosowana do kamer analogowych. Dodatkowo możemy analizować wiek, płeć, a nawet stan emocjonalny, aby łatwiej odnaleźć poszukiwaną osobę, a także przeprowadzać badania demograficzne, np. w celach marketingowych. Na przykład odszukanie nagrania, na którym widoczny jest mężczyzna z brodą i w okularach, nie zajmuje już wielu godzin mozolnej pracy, a zaledwie kilka chwil. Co więcej, opisywana seria rejestratorów za pomocą sztucznej inteligencji klasyfikuje obiekty w kategoriach człowiek/pojazd i przypisuje im szereg cech. W przypadku człowieka rozpoznawany jest kolor i typ ubioru (długi albo krótki rękaw, spodnie, krótkie spodenki, spódnica, czapka). Podczas wyszukiwania konkretnych pojazdów możliwe jest określenie rodzaju pojazdu (samochód czy jednoślad) i jego koloru, a jeśli w zasięgu kamery jest jego kierowca – sprawdzenie, czy zapiął pasy i czy nie rozmawia przez telefon.

Do serii AI należą rejestratory 16-kanałowe z miejscem na dwa dyski (**NVR5216-8P/16P-I**), a także 32-kanałowe z miejscem na cztery, a nawet osiem dysków twardych, obsługujące 32 i 64 kanały wizyjne (odpowiednio **NVR5432-16P-I, NVR5832/5864-I**).

Bezpośr. inf. Jacek Węglarz
Dahua Technology Poland

Funkcja RAID
w rejestratorach serii 6000

Nowy model rejestratora **NVR-6332-H8/FR** ma **funkcję RAID** rekomendowaną dla obiektów o wyższych standardach bezpieczeństwa przechowywanych danych.

Zastosowanie RAID, w zależności od konfiguracji, pozwoli zwiększyć niezawodność systemu (odporność na awarię dysku) oraz wydajność zespołu dysków, a także powiększyć przestrzeń dyskową dostępną jako jedna całość.

W rejestratorze można zainstalować do ośmiu dysków twardych i stworzyć tryb zapisu RAID. Dodatkowo rejestrator jest wyposażony w dwa zewnętrzne złącza eSATA do podłączenia pojedynczych twardych dysków służących do standardowego zapisu strumieni wizyjnych z kamer.

Wśród dostępnych trybów RAID są m.in. RAID 0 (*stripping*), RAID 1 (zapis lustrzany równolegle na dwóch zespołach dysków), RAID 5 (najczęściej wykorzystywany, gwarantujący bezpieczeństwo danych kosztem tylko jednego dysku) oraz RAID 6 (dający większą niezawodność niż RAID 5 kosztem dwóch dysków w systemie – awaria dwóch dowolnych dysków w tym samym czasie nie powoduje utraty danych). Dodatkowo administrator systemu może ustawić wybrany dysk lub dyski jako zapasowe, które automatycznie przejmą zadania uszkodzonego dysku. Kontroler RAID pozwala na zbudowanie kilku macierzy RAID i przyporządkowanie do nich wybranych kamer. Umożliwi to administratorowi podział systemu na partycje, a także wydzielenie kamer krytycznych (i uodpornienie pochodzących z nich danych na awarię dysku) oraz kamer standardowych – bez takiego zabezpieczenia.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Przełączniki sieciowe marki NOVUS
rekomendowane do systemów VSS i KD

Wszystkie modele przełączników są zgodne ze standardem **IEEE802.3af** i umożliwiają zasilanie podłączonych urządzeń **metodą PoE**. Moc, jaka może być pobrana z każdego z portów sieciowych, znacznie przekracza minimalną wartość narzuconą przez standard i dochodzi do 30 W. Zarządzalne modele przełączników są zgodne ze standardem IEEE802.3at (PoE+) i umożliwiają zasilanie urządzeń pobierających moc do 38 W. Zapewnia to wszechstronność w zasilaniu urządzeń o dużych poborach mocy (wyposażonych w promienniki podczerwieni, grzałki etc.). W celu zwiększenia dopuszczalnej długości kabli do transmisji danych oraz zasilania urządzeń wybrane modele mogą pracować w trybie rozszerzonym. Tryb ten umożliwia transmisję danych i zasilanie urządzeń nawet na odległość 250 metrów kosztem redukcji pasma transmisji do 10 Mbit/s, co w przypadku kamer o rozdzielczości do 6 Mpx nie powoduje żadnego ograniczenia parametrów. Dzięki trybowi rozszerzonemu można uprościć okablowanie i wyeliminować urządzenia pośredniczące. Modele 16- oraz 24-kanałowe mają światłowodowe porty Uplink, które są przydatne w obiektach, w których odległości między urządzeniami peryferyjnymi a przełącznikami przekraczają 250 metrów.

Przełączniki mają funkcje zwiększające odporność na nieuprawniony dostęp do zasobów systemu. Funkcja VLAN pozwala na wydzielenie fragmentów sieci dla różnych urządzeń z użyciem protokołu 802.1x (*one key VLAN*) lub przez bezpośrednie odseparowanie portów w przełączniku. Inne związane z bezpieczeństwem funkcje przełączników to Link Aggregation – redundancja połączenia, STP/RSTP (Spanning Tree Protocol) – zabezpieczenie przed zapętleniem sieci w systemie rozbudowanym, a także MAC Binding – przypisanie wybranego adresu MAC do wybranego portu przełącznika.

Bezpośr. inf. Patryk Gańko
AAT HOLDING

Depozytor kluczy
w ofercie firmy ROGER

Depozytor kluczy RKD32 jest elementem elektronicznego systemu dystrybucji i monitorowania obiegu kluczy. Każdy klucz znajdujący się w depozytorze podlega monitorowaniu i jest trwale zespolony z brelokiem zawierającym niepowtarzalny identyfikator zbliżeniowy RFID. Zespolenie klucza z brelokiem jest dokonywane przez użytkownika systemu i nie wymaga dodatkowych narzędzi ani zewnętrznych plomb. Klucze są przechowywane w 32 gniazdach z mechaniczną blokadą wyjęcia. Tylko uprawnieni użytkownicy mogą pobrać klucz w przedziale czasowym określonym w *Harmonogramach czasowych*. Użytkownicy systemu są identyfikowani po przyłożeniu kart zbliżeniowych lub podaniu kodów PIN. W *Trybie biurowym* depozytora można swobodnie pobierać i zwracać klucze bez konieczności identyfikacji użytkownika. Użytkownicy systemu mogą zarezerwować klucze na określony dzień i godzinę. System może powiadamiać o rezerwacji klucza lub blokować jego pobranie. W przypadku awarii depozytora możliwe jest komisyjne otwarcie obudowy i odblokowanie wszystkich kluczy za pomocą przycisku awaryjnego. System rejestruje czas pobrania i zwrotu klucza, a także to, kto wykonał daną czynność. Otwarcie drzwi depozytora z pominięciem identyfikacji użytkownika, a także próba ingerencji w jego wnętrze są rejestrowane i mogą być sygnalizowane przez sygnalizator optyczno-akustyczny systemu alarmowego. Program zarządzający ma prosty i czytelny interfejs użytkownika, który umożliwia prawidłową obsługę urządzenia po krótkim instruktażu. Depozytory RKD32 mogą pracować autonomicznie lub być elementem systemu kontroli dostępu i automatyki budynkowej RACS 5. Depozytory RKD32 można łączyć w grupy, które są obsługiwane za pomocą tego samego panelu kontrolnego.

Bezpośr. inf. ROGER

Uproszczona wersja systemu RACS 5
w ofercie firmy ROGER

RACS 5 LT jest uproszczoną wersją systemu RACS 5 przeznaczoną do zastosowania w małych i średnich instalacjach systemów kontroli dostępu, w których wymagane są typowe funkcje związane z elektroniczną kontrolą ruchu osób w obiekcie. W systemie RACS 5 LT mogą być wykorzystane wyłącznie przeznaczone do tego kontrolery dostępu serii MC16LT. Kontrolery te współpracują ze standardowymi czytnikami i ekspanderami systemu RACS 5 podłączonymi do magistrali RS485 (z terminalami MCT i ekspanderami MCX), z czytnikami z interfejsem Wiegand, a także z zamkami bezprzewodowymi serii RWL (firmy ROGER). W każdym momencie możliwa jest aktualizacja zarówno licencji kontrolerów MC16LT, jak i wersji systemu do RACS 5 ST lub RACS 5 EX. Do obsługi systemu RACS 5 LT wymagany jest program VISO LT. Program ten ma prosty i czytelny dla użytkownika interfejs, co ułatwia jego obsługę, a także skraca czas potrzebny na konfigurację systemu na etapie instalacji. W RACS 5 LT dostępne są funkcje automatyki budynkowej wykorzystujące węzły automatyki oraz możliwość integrowania stref alarmowych systemu antywłamaniowego z systemem kontroli dostępu. Integracja z systemem alarmowym umożliwia prezentację stanów stref alarmowych na czytnikach kontroli dostępu, a także sterowanie stanem tych stref z poziomu tych czytników. Inne dostępne funkcje systemu RACS 5 LT to m.in. monitorowanie pracy systemu w czasie rzeczywistym, monitorowanie osób przebywających w dowolnie zdefiniowanych obszarach obiektu, mierzenie czasu przebywania użytkowników w tych obszarach, a także rejestracja zdarzeń z uwzględnieniem tzw. trybów RCP. RACS 5 LT jest zintegrowany z wybranymi modelami rejestratorów dostępnych na naszym rynku i umożliwia pobieranie zdjęć oraz nagrań wideo powiązanych ze zdarzeniami, które wystąpiły w systemie, jak również podgląd na żywo obrazu z kamer.

Bezpośr. inf. ROGER

Seminarium oraz konkurs Wydziału Elektroniki WAT

o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa po raz czwarty

19 lutego 2019 w Instytucie Systemów Elektronicznych (ISE) Wydziału Elektroniki WAT odbyła się czwarta edycja seminarium dla studentów i kadry naukowo-dydaktycznej. W tym czasie zorganizowany został także konkurs o tytuł Mistrza Elektronicznych Systemów Bezpieczeństwa dla studentów Wydziału Elektroniki (specjalności inżynieria systemów bezpieczeństwa). W seminarium oraz konkursie wzięły udział firmy z branży elektronicznych systemów bezpieczeństwa. W konkursie wzięło udział 41 studentów, a jego zwycięzcą został **Adrian Błażejczak** – student II roku studiów stacjonarnych II stopnia na kierunku elektronika i telekomunikacja (specjalność: inżynieria systemów bezpieczeństwa). Tytuł pierwszego wicemistrza wywalczył **Jan Majewski**, a drugiego – **Kamil Krzemiński**. Wyróżniono także siedmiu innych uczestników. Największy znawca elektronicznych systemów zabezpieczeń Adrian Błażejczyk otrzymał okolicznościową statuetkę oraz nagrodę w formie kursu specjalistycznego ufundowanego przez Polską Izbę Systemów Alarmowych. Zwycięzcy i wyróżnieni otrzymali pamiątkowe dyplomy oraz upominki od firm uczestniczących w wydarzeniu.

– *Spotkanie studentów z przedstawicielami firm branżowych to doskonała okazja do zapoznania się z zapotrzebowaniem na rynku pracy. Zależy nam, aby studenci podczas tego wydarzenia mogli wybrać jak najlepsze miejsca pracy, a pracodawcy odnaleźli tu swoich przyszłych pracowników* – powiedział dziekan Wydziału Elektroniki prof. dr hab. inż. Andrzej Dobrowolski. Witając gości, dyrektor Instytutu Systemów Elektronicznych na Wydziale Elektroniki dr hab. inż. Zbigniew Watral podkreślił, że większość współpracujących z Akademią firm uczestniczy w każdej edycji seminarium. – *Spotykamy się już czwarty raz. Cieszy nas to, że liczba firm prezentujących swój dorobek i uczestniczących w seminarium jest coraz większa* – powiedział dyrektor. W ramach podziękowania za zaufanie i wieloletnią współpracę firma SATEL została wyróżniona przez Radę Wydzia-

łu Elektroniki Medalem za Zasługi dla Wydziału Elektroniki Wojskowej Akademii Technicznej. Seminarium rozpoczęli studenci, którzy zaprezentowali swoją działalność i osiągnięcia w Kole Naukowym Elektroników. Opiekun Koła i jednocześnie zastępca dyrektora ISE dr inż. Michał Wiśnios opowiedział o realizowanych przez studentów projektach oraz sukcesach na licznych targach branżowych. Na seminarium była też wystawa prac studentów Wydziału Elektroniki.

W każdej edycji seminarium biorą udział czołowe firmy z branży, z którymi Wydział Elektroniki podpisał porozumienia o współpracy. W tegorocznej edycji udział wzięło 10 firm: Bosch, SATEL, Pulsar, AAT HOLDING, POLON-ALFA, ICS Polska, Schrack Seconet, MR System, Janex i PISA. Przedstawiciele firm zaprezentowali swoje produkty oraz najnowsze rozwiązania z dziedziny elektronicznych systemów bezpieczeństwa. Wystąpienia obejmowały prezentacje dotyczące obecnego stanu rozwiązań technicznych z dziedziny inteligentnych systemów bezpieczeństwa. Podano przykłady ich zastosowań. Seminarium było przeznaczone głównie dla pracowników naukowo-dydaktycznych Instytutu i studentów specjalności inżynieria systemów bezpieczeństwa.

Efekty współpracy Wydziału Elektroniki z firmami branżowymi są widoczne. Studenci znajdują zatrudnienie w firmach oraz organizują specjalistyczne praktyki. Warto również wspomnieć o czterech laboratoriach Wydziału Elektroniki, które zostały wyposażone w specjalistyczny sprzęt przez firmy AAT HOLDING, Bosch, Janex International, POLON-ALFA, Pulsar, SATEL i Schrack Seconet. W pracowniach dydaktycznych kształcą się studenci specjalności inżynieria systemów bezpieczeństwa na kierunku elektronika i telekomunikacja.

Bezpośr. inf.
dr hab. inż. Jacek Paś
Wojskowa Akademia Techniczna
Wydział Elektroniki
Instytut Systemów Elektronicznych
Zakład Eksploatacji Systemów Elektronicznych

Ewakuacja osób niepełnosprawnych z budynków wysokich

Jan Dziedzic

Osoby niepełnosprawne nie mają łatwego życia. Jednym z rodzajów niepełnosprawności jest tzw. niepełnosprawność ruchowa. Ustawa *Prawo budowlane* z 7 lipca 1994 r. (Dz. U. z 2018 r., poz. 1202 z późn. zm.) wymusza stosowanie w budynkach różnych rozwiązań technicznych, które mają ułatwić niepełnosprawnym funkcjonowanie, w tym przemieszczanie się. Niestety rozwiązania te nie są w stanie im pomóc, gdy w budynku dojdzie do pożaru. Jakie działania można podjąć, aby bezpiecznie, szybko i łatwo ewakuować osoby niepełnosprawne?

Ewakuacja osób niepełnosprawnych jest opisywana w instrukcjach dotyczących bezpieczeństwa pożarowego obiektu. W większości instrukcji znajduje się opis metod ewakuacji obejmujących wyprowadzenie przez jedną lub dwie osoby oraz przenoszenie przez jedną lub dwie osoby – różnymi sposobami (często jest to przedstawione graficznie, jak na rysunku 1.). Należy jednak zadać sobie kilka pytań:

1. Czy użytkownicy obiektu (najemcy) czytają instrukcje dotyczące bezpieczeństwa pożarowego?
2. Czy skorzystają oni z informacji zawartych w instrukcji czy pomogą „po swojemu”?
3. Czy w ogóle będą skłonni do pomocy?
4. Czy takie sposoby ewakuacji są ćwiczone?
5. Czy jest inny sposób ewakuacji osób niepełnosprawnych?

Na podstawie doświadczeń autora można odpowiedzieć następująco: ad 1 – sporadycznie albo wcale; ad 2 – raczej będą improwizować (ponieważ nie czytają instrukcji); ad 3 – tak, o ile zagrożenie nie będzie bezpośrednie, bliskie, wyczuwalne; ad 4 – nie, nie są ćwiczone; ad 5 – tak, można wykorzystać windę pożarową.

Zgodnie z rozporządzeniem Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 15 czerwca 2002 r. z późn. zm.) w budynkach wysokich i wysokościowych ZL I, ZL II, ZL III i ZL V przynajmniej jeden dźwig (winda) powinien być przystosowany do potrzeb ekip ratowniczych. Windy takie powinny spełniać wymagania zawarte w normie PN-EN 81- 72:2005 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Szczególne zastosowania dźwigów osobowych i towarowych – Część 72: Dźwigi dla straży pożarnej* lub w obowiązującej od 2015 r. normie

Rys. 1. Sposoby ewakuacji osób niepełnosprawnych (sprowadzanie i przenoszenie)

PN-EN 81-72:2015-06 *Przepisy bezpieczeństwa dotyczące budowy i instalowania dźwigów – Szczególne zastosowania dźwigów osobowych i towarowych – Część 72: Dźwigi dla straży pożarnej*, a ich głównym zadaniem jest dowiezienie ekip ratowniczych na dowolną kondygnację budynku, co oznacza, że mogą być wykorzystane w działaniach ratowniczych (podczas pożaru w budynku).

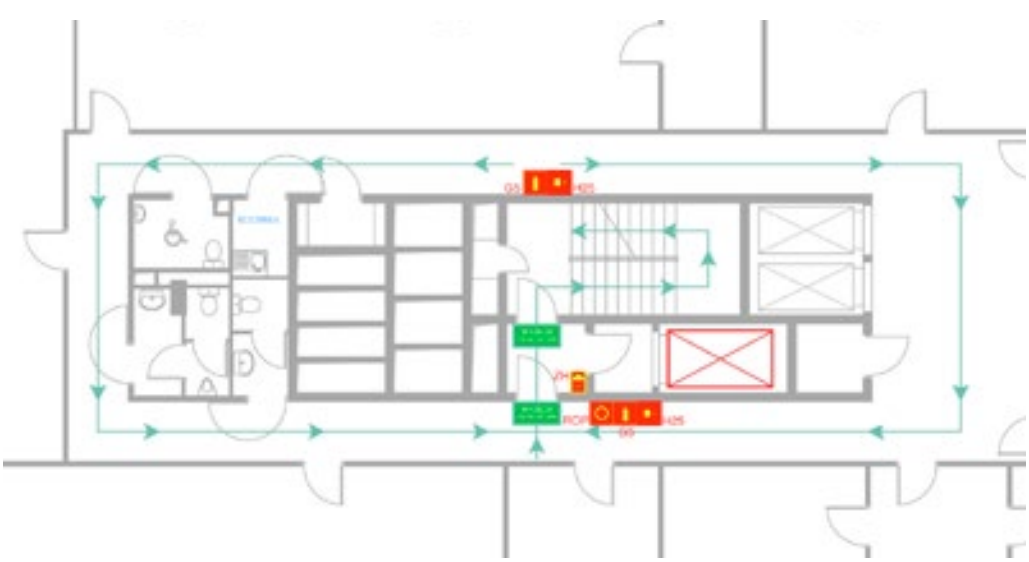
Standardowo w budynkach wysokich i wysokościowych w Polsce (a także w większości krajów Europy) wszystkie windy najczęściej zostają sprowadzone w przypadku pożaru na parter. Jedynie winda dla ekip ratowniczych (pożarowa) może być wykorzystana do przewożenia ludzi i sprzętu (jeździ podczas pożaru). Czy można tę windę wykorzystać do ewakuacji?

Czy jest to jedyna możliwość ewakuacji osób niepełnosprawnych? Jak można przygotować budynek na wypadek ewakuacji osób niepełnosprawnych?

Optymalne rozwiązanie

Budynek powinien być wyposażony w zgodną z przepisami i normami windę pożarową z przedsionkami przeciwpożarowymi na każdej kondygnacji budynku. Winda pożarowa powinna być dostępna na wszystkich kondygnacjach budynku – także na kondygnacjach garażowych.

Szyb windy pożarowej powinien być usytuowany w takim miejscu w budynku, by przedsionek przeciwpożarowy windy przylegał do przedsionka przeciwpożarowego ewakuacyjnej klatki schodowej (rys. 2.) lub przedsionek przeciwpożarowy windy pożarowej był jednocześnie przedsionkiem przeciwpożarowym ewakuacyjnej klatki schodowej (rys. 3.). Nie wiadomo (to kwestia interpretacji), czy można zastosować wspólny przedsionek przeciwpożarowy dla windy pożarowej i klatki schodowej.

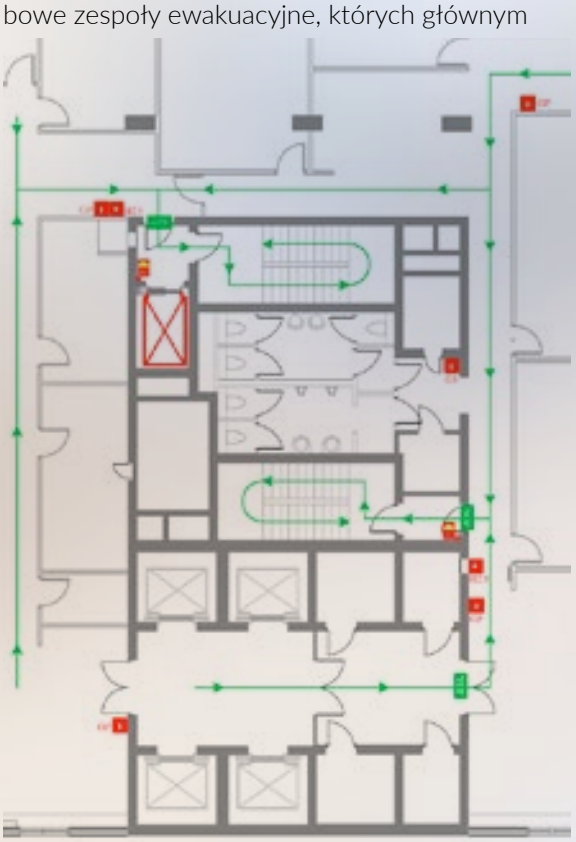


Rys. 2. Winda pożarowa z dodatkowym, własnym przedsionkiem przeciwpożarowym

Budynek powinien być wyposażony w certyfikowany system telefonów pożarowych z aparatami telefonicznymi w przedsionku przeciwpożarowym klatki schodowej lub w przedsionku windy pożarowej.

Do personelu zajmującego się ochroną budynku należy/może należeć strażak dyżurny, którym jest funkcjonariusz PSP (nadal pełniący służbę w jednostce PSP lub emerytowany). W przypadku braku takiego stanowiska w danym miejscu ochroniarze powinni być przeszkoleni w zakresie obsługi systemów przeciwpożarowych budynku, w tym jazdy windą pożarową (jeżdżenie windą pożarową powinno się ćwiczyć, np. w każdą sobotę i niedzielę). Jeżeli personel zajmujący się ochroną jest liczny, jedna osoba (strażak dyżurny) wykonuje polecenia kierującego działaniami ratowniczymi (KDR), czyli dowodzącego strażakami przybyłymi na miejsce pożaru, a także obsługuje windę pożarową.

U wszystkich najemców, na każdej kondygnacji budynku, powinny być wyznaczone kilkuosobowe zespoły ewakuacyjne, których głównym zadaniem ma być przeprowadzenie sprawnej ewakuacji, czyli skierowanie osób przebywających na zagrożonej kondygnacji do wyjść ewakuacyjnych i udzielenie pomocy osobom jej potrzebującym (np. niepełnosprawnym lub osobom, które zasłabły). Jeżeli nie występuje bezpośrednie zagrożenie dla zdrowia i życia (nie ma płomieni, dymu itp.) członkowie zespołów ewakuacyjnych powinni sprawdzić wszystkie pomieszczenia i upewnić się, że nikt z pracowników i gości nie został na danej kondygnacji. Pomoc osobom jej potrzebującym może polegać na doprowadzeniu ich, ewentualnie dowiezieniu (na wózku, krześle biurowym z kółkami itp.) i przeniesieniu do przedsionka windy pożarowej albo klatki schodowej, a także na powiadomieniu przez telefon pożarowy personelu zajmującego się ochroną (członek zespołu ewakuacyjnego opiekuje się osobą potrzebującą pomocy do przyjazdu windy pożarowej lub do przybycia strażaków z PSP).



Rys. 3. Winda pożarowa z przedsionkiem przeciwpożarowym wspólnym z klatką schodową

Uwaga! Zespoły ewakuacyjne nie prowadzą działań na kondygnacjach garażowych, na których także mogą (w momencie rozpoczęcia ewakuacji) przebywać osoby niepełnosprawne. Na tych kondygnacjach osoby niepełnosprawne powinny samodzielnie udać się do przedsionka przeciwpożarowego klatki schodowej lub windy pożarowej i wezwać pomoc, korzystając z telefonu pożarowego.

W przypadku alarmu pożarowego drugiego stopnia i ewakuacji zagrożonej kondygnacji strażak dyżurny lub pracownik ochrony oczekuje na przyjazd jednostek PSP i obserwuje centrale systemów przeciwpożarowych (SAP i DSO), a także panel przeznaczony do obsługi systemu telefonów pożarowych.

W tym miejscu należy wspomnieć, że jednym z najczęściej spotykanych scenariuszy pożarowych dotyczących budynków wysokich i wysokościowych jest scenariusz zakładający ewakuację kondygnacji zagrożonej lub objętej pożarem oraz kondygnacji garażowych i technicznych budynku. Postępowanie zgodnie z takim scenariuszem polega m.in. na nadawaniu komunikatów ewakuacyjnych na zagrożonej kondygnacji, na kondygnacjach garażowych i technicznych, a także na klatce lub klatkach schodowych. Na pozostałych kondygnacjach (wszystkich) nadawane są komunikaty ostrzegawcze.

Podczas oczekiwania na przyjazd jednostek PSP strażak dyżurny lub pracownik ochrony odbiera ewentualne połączenia z systemu telefonów pożarowych. Jeżeli przychodzą zgłoszenia dotyczące konieczności udzielenia pomocy osobie niepełnosprawnej lub takiej, która nie jest w stanie opuścić budynku klatką schodową, odnotowuje je (telefony są adresowalne), aby przekazać informacje KDR-owi.

Od tego momentu to KDR decyduje o wszelkich działaniach ratowniczo-gaśniczych w budynku. Należy podkreślić, że strażacy z PSP w pierwszej kolejności upewnią się, że pożar nie zagraża bezpośrednio osobom przebywającym w budynku, a jeżeli tak, to podejmą czynności w celu ewakuacji osób zagrożonych. Jeżeli po zapoznaniu się z sytuacją KDR zadecyduje o ewakuacji osób niepełnosprawnych, może wykorzystać windę pożarową obsługiwaną przez strażaka dyżurnego lub pracownika ochrony do ewakuacji takich osób i jednoczesnego dowiezienia strażaków z PSP i sprzętu na zagrożoną kondygnację.

Dzięki systemom przeciwpożarowym w budynkach wysokich i wysokościowych (m.in. nawiewowi do szybu windy pożarowej, nawiewowi do przedsionka przeciwpożarowego zagrożonej kondygnacji, drzwiom przeciwpożarowym przedsionka klatki schodowej i ewentualnie przedsionka windy pożarowej) ani strażakom z PSP, ani strażakowi dyżurnemu lub pracownikowi ochrony obsługującemu windę nic nie powinno zagrażać. Również osoba niepełnosprawna i jej opiekun z zespołu ewakuacyjnego mogą niezagrożeni czekać na pomoc przez 30 minut w przedsionku przeciwpożarowym klatki schodowej lub 60 minut w przedsionku windy pożarowej w budynku wysokim, a w budynku wysokościowym przez 60 minut w przedsionku przeciwpożarowym klatki schodowej lub 120 minut w przedsionku windy pożarowej.

W przypadku konieczności ewakuacji całego budynku (np. z powodu alarmu bombowego) można wykorzystać do ewakuacji osób niepełnosprawnych również windę pożarową. W przypadku alarmu bombowego KDR-rem jest funkcjonariusz policji i to on decyduje o wszelkich działaniach w budynku. Strażak dyżurny lub pracownik ochrony może odmówić udziału w ewakuacji z wykorzystaniem windy pożarowej. Wówczas KDR powinien wyznaczyć funkcjonariusza policji lub poprosić o pomoc funkcjonariuszy PSP. W większości przypadków personel w budynku udzieli KDR-owi pomocy. W skrajnej sytuacji windą pożarową można zabrać nawet kilka osób niepełnosprawnych (z ich opiekunami) z różnych kondygnacji, a nawet zrobić to kilka razy. Takie przypadki z różnych względów nie są ujawniane i opisywane w środkach masowego przekazu. W niektórych budynkach ćwiczy się ewakuację z wykorzystaniem windy pożarowej w ramach obowiązkowych ćwiczeń ewakuacyjnych (raz w roku – ewakuuje się ludzi z całego budynku jednocześnie), według wcześniej przygotowanego, specjalnego scenariusza ćwiczeń (zespoły ewakuacyjne zgłaszają przez telefony pożarowe konieczność udzielenia pomocy osobom niepełnosprawnym lub symulującym niepełnosprawność). Po upewnieniu się, że na ćwiczenia ewakuacyjne nie przyjadą jednostki PSP (po odczekaniu ok. 5–10 minut) strażak dyżurny realizuje procedurę ewakuacji z wykorzystaniem windy pożarowej, zabierając osoby oczekujące na pomoc z jednej lub kilku kondygnacji.

W odpowiednio wykonanym i wyposażonym budynku wysokim lub wysokościowym kategorii ZL III można już dziś wykorzystać windę pożarową do ewakuacji osób niepełnosprawnych.

Rozwiązaniem alternatywnym, wynikającym z rozporządzenia Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 15 czerwca 2002 r. z późn. zm.), jest ewakuacja do sąsiedniej strefy pożarowej. W przypadku budynku wysokiego czy wysokościowego, w którym działa się zgodnie ze scenariuszem pożarowym wymuszającym ewakuację tylko jednej zagrożonej kondygnacji, formalnie można ewakuować jedną lub wiele osób (w tym osoby niepełnosprawne) na sąsied-

Artykuł jest skierowany do:

- **właścicieli i administratorów budynków**
(mają wpływ na wyposażenie budynku i działalność personelu zajmującego się jego ochroną),

- **prezesów i dyrektorów firm**
wynajmujących powierzchnie w budynkach wysokich lub wysokościowych (wiedzą oni o osobach niepełnosprawnych, które u nich pracują, a także mają wpływ na skład zespołów ewakuacyjnych i doskonalenie przez nie umiejętności),

- **architektów**
(mogą zaprojektować odpowiednie rozwiązania uwzględniające windy pożarowe i wyposażenie budynku),

- **firm oferujących ochronę obiektów**
(mogą one zaproponować rozszerzoną ofertę usług),

- **użytkowników (najemców) obiektów**
(powinni oni wiedzieć, jak przeprowadzać ewakuację w budynku i tego, jakiej pomocy mogą się spodziewać).

nią – najlepiej niższą – kondygnację (do sąsiedniej strefy pożarowej). Warunkiem dopuszczającym ewakuację osób na inną kondygnację jest niedopuszczenie do przekroczenia maksymalnej dopuszczalnej liczby osób na niezagrożonej kondygnacji. O takich możliwościach ewakuacji w ogóle się nie mówi, a poza tym w komunikatach z dźwiękowych systemów ostrzegawczych (DSO) jest prośba o opuszczenie budynku najbliższym wyjściem ewakuacyjnym, a więc nie ma informacji o ewentualnej ewakuacji do sąsiedniej strefy pożarowej.

Zgodnie z tymi samymi przepisami za przeprowadzoną (zrealizowaną) ewakuację należy uznać wyście na wentylowaną (pożarowo) klatkę schodową, oddzieloną od pozostałej części budynku przedsionkiem przeciwpożarowym.

Ze względu na to, że w typowym wysokim lub wysokościowym budynku biurowym na jednej kondygnacji przebywa średnio jedna osoba niepełnosprawna, ewakuacja takiej osoby z kondygnacji zagrożonej do sąsiedniej powinna być nie tylko możliwa, ale wręcz zalecana. Jest możliwa nawet w budynku wyposażonym w rozbudowane systemy kontroli dostępu, które zazwyczaj są odłączane we wszystkich drzwiach ewakuacyjnych w budynku, niezależnie od miejsca pożaru.

Swoją drogą należałoby zastanowić się nad oznaczaniem/wyróżnianiem takich budynków, aby KDR dojeżdżający na miejsce pożaru wiedział, jaką pomoc może uzyskać od służb budynkowych.

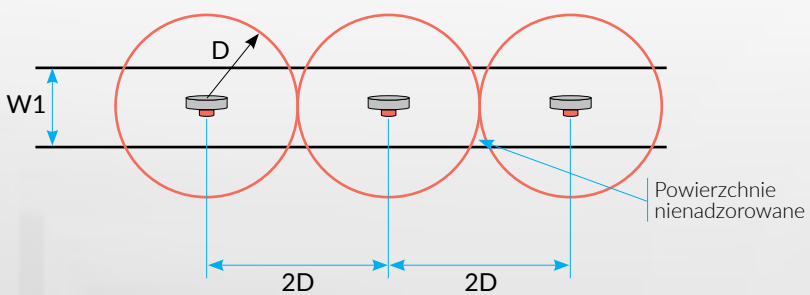
Jan Dziedzic

Czujki pożarowe
w wąskich pomieszczeniach

mgr inż. Jerzy Ciszewski

Wąski korytarz

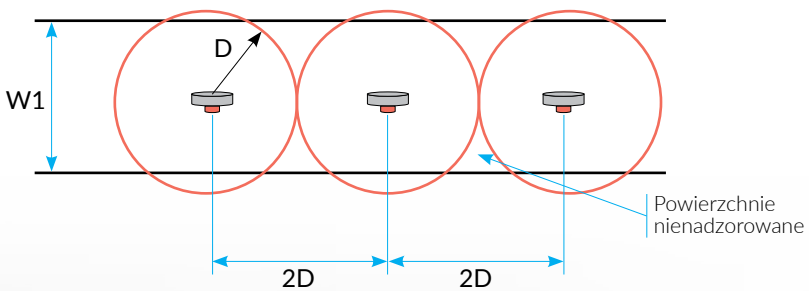
Może wydawać się, że wąskie pomieszczenia, np. korytarze, nie mogą nastręczać istotnych problemów z rozmieszczeniem czujek pożarowych. Tak jest w istocie, jednak pod pewnymi warunkami. Na rysunku 1 pokazano nadzorowanie wąskiego pomieszczenia zgodne z zasadą, jaką zalecają różne wytyczne projektowania. Ponieważ odległość między czujkami wynosi 2D, zasięgi czujek w formie okręgów są styczne. Przyjmując dostatecznie małą szerokość pomieszczenia W1, można stwierdzić, że praktycznie cała jego powierzchnia jest skutecznie nadzorowana tak, jak na rysunku 1.



Rys. 1. Skuteczny nadzór wąskiego pomieszczenia/korytarza o szerokości W1 z wykorzystaniem czujek

Przyjmuje się, że, mimo braku zasięgu na skutek stosunkowo małej szerokości pomieszczenia, dym, nie mogąc przemieszczać się w poprzek pomieszczenia, niejako uzupełnia braki w zasięgu czujki, wypełniając małe przestrzenie nienadzorowane. Należy w związku z tym ustalić, przy jakiej minimalnej szerokości pomieszczenia możliwe jest nadzorowanie zgodne z rysunkiem 1.

Sytuacja jest zupełnie inna, gdy szerokość pomieszczenia jest większa. W takim przypadku nadzorem nie są objęte duże przestrzenie, tak jak na rysunku 2.



Rys. 2. Niedostateczny nadzór szerokiego korytarza o szerokości W2 z wykorzystaniem czujek

Porównanie wymagań zawartych w metodykach projektowania

Poszczególne wytyczne dotyczące projektowania różnią się podanym zasięgiem czujek, a także wartością szerokości W, w przypadku której można zastosować przedstawioną na rysunku zasadę styczności zasięgów czujek.

W tabelach nr 1 i nr 2 podane są zasięgi czujek, odległości między nimi oraz maksymalne szerokości pomieszczeń/korytarzy. W tabeli 1 znajdują się dane dotyczące punktowej czujki dymu i otworów systemów zasysających. Z kolei zawartość tabeli 2 dotyczy punktowych czujek ciepła. Proszę

Wytyczne dotyczące projektowania	Zasięg czujki D [m]	Odległość między czujkami	Szerokość pomieszczenia W [m]
SITP WP-02:2010, pkt 4.5.4	7,5	2D	3
PKN-CEN TS54-14:2006	7,5	2D	3
BS 5839-1:2013, pkt 2.22.3	7,5	2D	2
prCEN TS-54-14:2018, pkt 6.5.2.3	6,2	2D	2
VdS 2095-2010-05 (07), pkt 6.2.7.5		15 m	3

Tab. 1. Punktowa czujka dymu

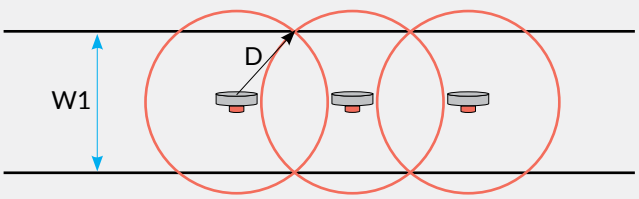
Wytyczne dotyczące projektowania	Zasięg czujki D [m]	Odległość między czujkami	Szerokość pomieszczenia W [m]
SITP WP-02:2010, pkt 4.5.4	5	2D	3
PKN CEN TS54-14:2006	5	2D	3
BS 5839-1:2013, pkt 2.22.3	7,5	2D	2
prCEN TS-54-14:2018, pkt 6.5.2.2	4,5	2D	2
VdS 2095-2010-05 (07), pkt 6.2.7.5		10 m	3

Tab. 2. Punktowa czujka ciepła

zwrócić uwagę na to, że nie podano w tabelach zasięgów dla wytycznych VdS 2095. Wynika to z przyjętej przez VdS stałej powierzchni przy rozmieszczaniu czujek.

Szeroki korytarz

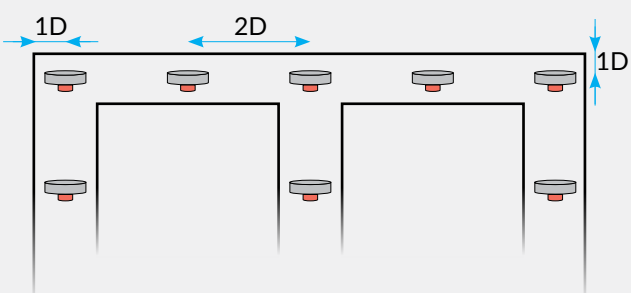
Jeżeli szerokość pomieszczenia przekracza wartości podane w tabelach nr 1 i nr 2, uznajemy je za pomieszczenie o dużej powierzchni. Należy wówczas przestrzegać zasad opisanych w artykule dotyczącym nadzorowania stropów płaskich. Zasada jest zilustrowana na rysunku 3.



Rys. 3. Sposób nadzoru szerokiego korytarza – podobny jak w przypadku dużych pomieszczeń

Rozmieszczenie czujek

Czujki należy rozmieścić w zależności od układu korytarza – z zasady na zakrętach i skrzyżowaniach korytarzy.

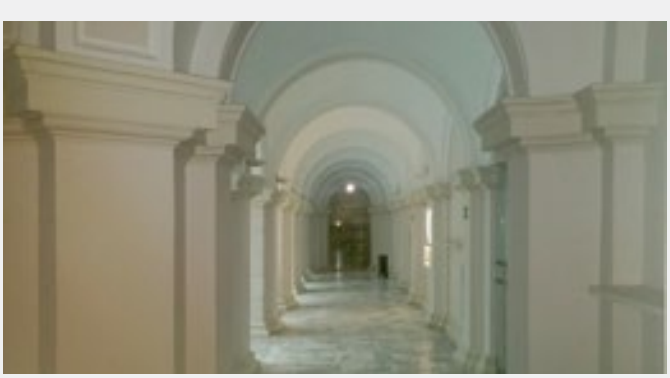


Rys. 4. Sposób rozmieszczenia czujek

Fot. 1. Sposób rozmieszczenia czujek liniowych

Nietypowy sposób nadzorowania korytarza – przykład

Na fotografiach nr 1 i nr 2 pokazano ciekawy sposób nadzoru wąskich korytarzy biegnących wokół krużganków Auli Dużej Politechniki Warszawskiej. Korytarze są nadzorowane liniowymi czujkami dymu wykorzystującymi lustra pryzmatyczne.



fot 2. Widok lustra liniowej czujki dymu zainstalowanego na końcu korytarza. Proszę zwrócić uwagę, że pryzmatyczne lustro odbiło światło (błyszczący punkt na fotografii) dokładnie w kierunku, z którego został wysłany impuls świetlny z lampy błyskowej.

Problematyczny sposób nadzorowania korytarza – przykład

Na fotografii 3 pokazany jest nadzór długiego korytarza z pasmem świetlnym wykonanym w formie stropu dwuspadowego. Proszę zwrócić uwagę na to, jak wybrano miejsca zainstalowania czujek pożarowych. Czujki są umieszczone w miejscu połączenia pionowej ściany z nachylonym stropem. Zostało to zaznaczone czerwoną strzałką.

Fot. 3. Przykład nieskutecznego nadzoru

Odległość między czujkami jest równa 2D, a więc przyjęto koncepcję stycznych zasięgów czujek, możliwą do zastosowania w wąskich korytarzach ze stropem płaskim, jednak w tym przypadku taki sposób nadzorowania może być nieskuteczny – dym może dotrzeć do układu pomiarowego czujki dopiero po wypełnieniu przestrzeni podstropowej, co ewidentnie nastąpi na skutek rozwoju pożaru.

Ze względu na wielkie przeszklenia stropu projektant prawdopodobnie brał pod uwagę możliwość powstawania dużej warstwy poduszki powietrznej wytwarzanej na skutek radiacji słonecznej. Nawet jeśli przyjmiemy powstanie poduszki powietrznej w dolnej części przeszklenia, czujka będzie znajdowała się praktycznie na krawędzi ściany oraz wirtualnego płaskiego stropu utworzonego przez gorące powietrze. Mocowanie czujek do przystropowej części ściany nie jest

Fot. 4. Przykład nieskutecznego nadzoru

prawidłowym rozwiązaniem. Minimalna odległość, mierzona w pionie i poziomie, to 50 cm. W przypadku stropu szedowego przeważnie wymaga się, aby czujki były zainstalowane w odległości ok. 60 cm od najwyższej części stropu. Sposób nadzorowania pod pilastym, dwuspadowym stropem jest zagadnieniem złożonym i jest opisany w osobnym artykule dotyczącym nadzorowania w przypadkach szczególnych ukształtowań stropu.

mgr inż. Jerzy Ciszewski
IBP NODEX

Bibliografia

1. *Wstęp do projektowania instalacji sygnalizacji pożarowej*, CNBOP 1996.
2. Wytyczne SITP WP-02:2010 *Instalacje sygnalizacji pożarowej. Projektowanie.*
3. PKN-CEN/TS 54-14:2006 *Systemy sygnalizacji pożarowej. Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji.*
4. prCEN/TS 54-14:2018 *Fire detection and fire alarm systems. Part 14: Guidelines for planning, design, installation, commissioning, use and maintenance.*
5. VdS 2095:2010-05(07) *VdS-Richtlinien für automatische Brandmeldeanlagen. Planung und Einbau.*
6. BS 5839-1:2013 *Fire detection and fire alarm systems for building. Part 1: Code of practice for system design, installation, commissioning and maintenance of systems in non-domestic premises.*
7. NFPA 72:2013 *National Fire Alarm and Signaling Code*

Zabezpieczanie składowisk materiałów oraz odpadów niebezpiecznych dla środowiska

Maciej Prelich

W ubiegłym roku wybuchło wiele pożarów w miejscach składowania odpadów. Takie pożary nie tylko zagrażają zwierzętom i roślinom, ale również powodują olbrzymie zanieczyszczenie powietrza i gleby. W maju 2018 r. na wysypisku w Zgierzu wybuchł pożar, który trwał tydzień, a w jego efekcie spłonęło ponad 50 tys. ton śmieci, w tym wiele odpadów toksycznych

Po tych wydarzeniach Minister Środowiska wprowadził nowe rozporządzenie nakazujące firmom obsługującym składowiska odpadów potencjalnie niebezpiecznych zainstalowanie systemu monitorowania umożliwiającego dozór miejsc magazynowania w dzień i w nocy. Wszystkie dane mają być zapisywane, a odpowiednie służby mają mieć możliwość podglądu w czasie rzeczywistym. Firmy miały sześć miesięcy na przygotowanie się przed wejściem rozporządzenia w życie pod koniec lutego. Jest to jednak dość mało czasu, jeśli weźmie się pod uwagę duże wymagania sprzętowe i miejsca usytuowania wielu ze składowisk – rozległe, często nieuzbrojone tereny o zmiennej topografii wynikającej z ciągłego użytkowania terenów.

Na tereny, gdzie składowane są odpady, włamują się zbieracze przedmiotów metalowych i innych surowców wtórnych, jednak koszty ochraniania terenu lub jego ogrodzenia zwykle przewyższają potencjalne korzyści. Utworzenie systemu kontroli wizyjnej jest jeszcze trudniejsze (oraz droższe), gdyż wspomniana wcześniej zmienna oraz skomplikowana rzeźba terenu często przyczynia się do zasłonięcia części obszaru i wymusza instalację systemu w jak najmniejszej odległości, co przekłada się na większe wymagania dotyczące obiektywów kamer.

Doświadczone firmy z branży zabezpieczeń, takie jak Firma ATLine sp.j. Sławomir Pruski, nie będą miały problemu ze skompletowaniem systemu odpowiadającego nowym przepisom. Zazwyczaj do obserwacji w ciemności służą kamery termowizyjne, jednak postęp techniki umożliwia nam zastosowanie kamer z podświetleniem podczerwonym opracowanym przed firmę Infiniti Electro-Optics z Kanady.

Podczerwień (ang. *infrared* – IR) to promieniowanie elektromagnetyczne, którego widmo mieści się w zakresie od 780 nm do około 1 mm, czyli od dolnej granicy światła widzialnego do mikrofal. To sprawia, że jest ono niewidzialne dla ludzkiego oka, ale może być odbierane przez przetwornik w kamerze i przekształcane w wyraźny czarno-biały obraz. LED-owe diody pracujące w podczerwieni są powszechnie stosowane w przemyśle, w wizyjnych systemach dozorowych, do oświetlania scen, które są zbyt ciemne, by mogły być obserwowane przez kamery pracujące w świetle widzialnym. Większość oświetlaczy diodowych ma jednak ograniczony zasięg, nie przekraczający 300 metrów. Aby wyjść poza ten zakres, firma Infiniti opracowała diodę laserową ZLID (Zoom Laser IR Diode).

Już w przeszłości firmy eksperymentowały z użyciem laserów do poprawy zasięgu oświetlenia podczerwonego, jednak z miernym efektem, głównie ze względu na użycie tanich podzespołów o zbyt niskiej jakości. Oświetlacz z diodami ZLID dostosowuje intensywność świecenia

Kamera umożliwi identyfikację znalezionych celów. Eliminując potrzebę zastosowania termowizji, można zmniejszyć wymagania budżetowe, a zasięg 5 km pozwala na obserwację dużego wycinka terenu za pomocą jednej kamery.

Fot. 1. Kamera Infiniti Electro-Optics Phoenix z diodami ZLID

i wielkość pola oświetlanego przez laser na zasadzie zmian ogniskowej układu optycznego kształtującego wiązkę światła. W ten sposób wyeliminowane zostaje prześwietlenie pewnych obszarów i powstawanie tak zwanych gorących punktów, które zwykle występują w laserach. Oświetlacze z diodami ZLID w połączeniu z precyzyjnie zaprojektowanymi układami optycznymi kamery są w stanie zapewnić równomierne oświetlenie, gwarantujące wytworzenie czystego obrazu w całkowitej ciemności, na odległość nawet do pięciu kilometrów. Dodatkowo ta metoda zapewnia widoczność przez szkło pomimo blokowania części fal z zakresu podczerwieni przez ten materiał.

Zastosowanie takich oświetlaczy ułatwia zastosowanie dozoru wizyjnego na terenach składowisk materiałów oraz odpadów. W celu osiągnięcia jeszcze większej skuteczności wykrywania intruzów na danym terenie kamery można połączyć z radarem, który będzie odpowiadał za detekcję.

Niestety nie jest to rozwiązanie idealne – ze względu na zastosowanie lasera nie jest wskazane zastosowanie tych kamer w miejscach, gdzie możliwy jest ruch pieszych w niebezpiecznie małej odległości. Wszystkie tego typu kamery mają wskaźnik NOHD (Nominal Ocular Hazard Distance). Oznacza to, że z pewnej odległości laser może spowodować trwałe pogorszenie wzroku, jeśli nie nosi się specjalnych okularów ochronnych. Nie istnieje jednak rozwiązanie idealne. Każda technika detekcji i każdy rodzaj kamery ma swoje zalety i wady, a dobranie jak najlepszych rozwiązań jest zadaniem dla integratorów. Eksperci Firma ATLine sp.j. Sławomir Pruski codziennie mierzą się z najbardziej wymagającymi projektami oraz starają się znaleźć najnowsze rozwiązania w branży, tak aby klienci byli w pełni zadowoleni ze swoich systemów.

Maciej Prelich
Firma ATLine sp.j. Sławomir Pruski
mprelich@atline.pl

NOVUS®

6000 VSS IP

NOVUS IP NMS Compatible ONVIF

SKUTECZNE ROZPOZNAWANIE TWARZY

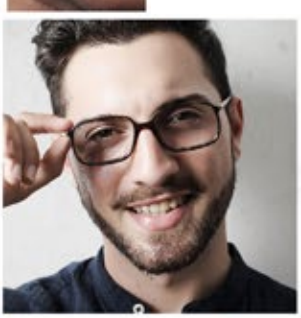
W REJESTRATORACH SERII 6000
W POŁĄCZENIU Z KAMERAMI SERII 6000

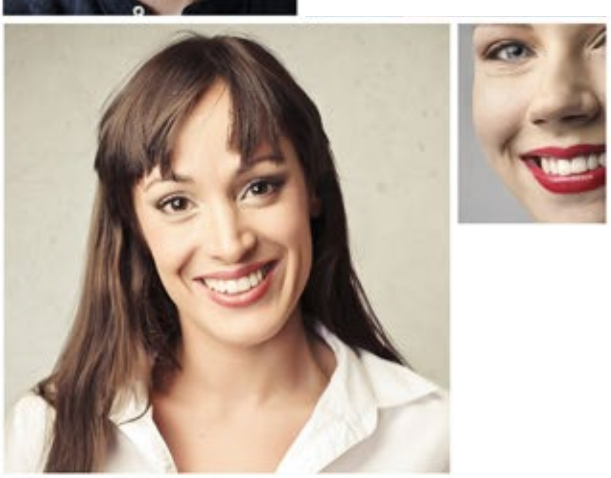
AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

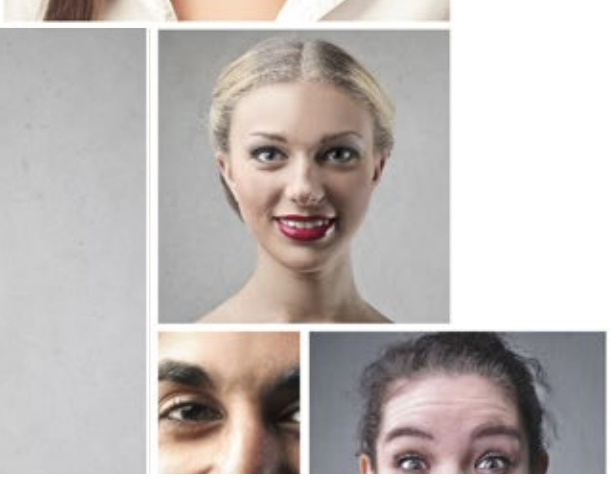
Rozpoznawanie twarzy

w systemach VSS marki NOVUS
Funkcje sieciowe

Patryk Gańko







W magazynie *Zabezpieczenia nr 4/2018* opublikowany został artykuł pt. *Rozpoznawanie twarzy w systemach VSS marki NOVUS*. Wykorzystanie funkcji rozpoznawania twarzy zostało ograniczone

Fot. 1. Baza danych twarzy

tylko do lokalnej obsługi wymagającej obecności administratora systemu bezpośrednio przed rejestratorem. Ta cecha mogła ograniczyć efektywne wykorzystanie tej funkcji w przypadku obiektów rozproszonych i równocześnie centralnie zarządzanych z wykorzystaniem protokołu TCP/IP. Świadom tej niedogodności producent intensywnie rozwijał moduł sieciowy. Wydanie nowych wersji oprogramowania dostosowanych do systemów operacyjnych Windows, Android i iOS wyeliminowało te utrudnienia. Ponieważ w niniejszym artykule chciałbym ograniczyć się do opisu opcji sieciowych funkcji rozpoznawania twarzy, zachęcam czytelników do przeczytania również archiwalnego artykułu, który nie zdezaktualizował się. Wymagania dotyczące montażu kamer i obrazu służącego rozpoznawaniu twarzy nie zmieniły się. Również zasady obsługi zachowują swą ważność. Zwiększono jedynie liczbę modeli rejestratorów z serii 6000 obsługujących funkcję rozpoznawania twarzy. Dla łatwiejszej selekcji zostały one wyodrębnione w nowej nomenklaturze przez dodanie litery *F* na końcu nazwy. Aby osiągnąć pełną precyzję wywodu, chciałbym nadmienić, że opisane poniżej funkcje są dostępne w wersji 3.4.5.81130 oprogramowania NVR-6000-Viewer oraz w aplikacji mobilnej SuperLive Plus w wersji 1.6.0.

Fot. 2. Wysyłanie bazy danych

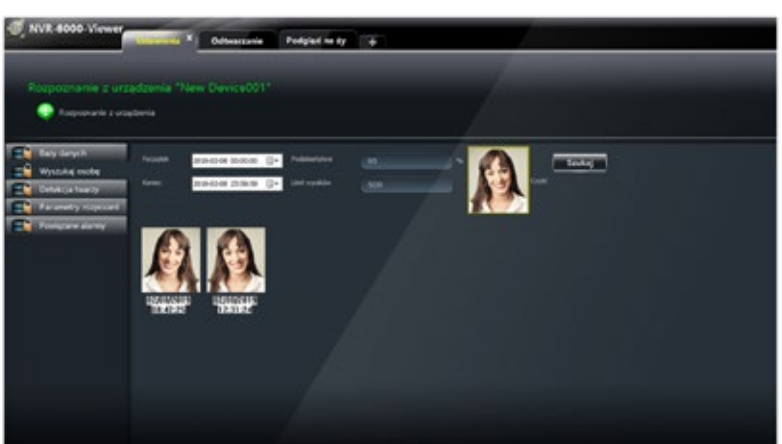
Po wybraniu rejestratora z listy urządzeń w aplikacji NVR-6000-Viewer i w menu *Rozpoznawanie twarzy* wyświetlony zostanie graficzny interfejs bazy danych twarzy (fot. 1).

Jest to baza danych zapisana w rejestratorze, do której użytkownik uzyskuje pełny zdalny dostęp. Administrator może dowolnie modyfikować, usuwać oraz tworzyć nowe grupy, a także dodawać lub usuwać wybrane osoby (rekordy). Nowym osobom w bazie mogą zostać przyporządkowane referencyjne widoki twarzy pochodzące z zewnętrznych źródeł (plików w formacie JPG) lub wizerunki zapisane w bazie danych rejestratora. Do każdej dodanej do bazy osoby mogą zostać przypisane dodatkowe dane – data i miejsce urodzenia, numer ID, numer telefonu i inne dane identyfikacyjne.

Poszczególne bazy danych mogą być poprzez sieć wysyłane do urządzeń obsługujących funkcję rozpoznawania twarzy, wskazanych w oprogramowaniu NVR-6000-Viewer (fot. 2). Daje to nowe możliwości zarządzania wieloma rozproszonymi obiektami w jednym centrum nadzoru i aktualizacji bazy danych dla wszystkich obiektów bez angażowania lokalnej obsługi i bez zbędnej zwłoki. Rozmowy z wieloma administratorami takich systemów (np. obejmujących sieć sklepów) wskazują na powtarzalność bezprawnych działań tych samych osób w wielu obiektach należących do sieci. Szybkie uaktualnienie bazy danych we wszystkich rejestratorach może być metodą prewencji i informowania w czasie rzeczywistym o potencjalnym zagrożeniu.

Wykrywanie twarzy jest możliwe po podłączeniu jakiejkolwiek kamery do rejestratora sieciowego z serii 6000 z funkcją rozpoznawania twarzy. Dzięki bardzo wysokiej wydajności systemu możliwe jest do 180 rozpoznań na minutę, w całym systemie. W aplikacji NVR-6000-Viewer administrator może określić przedział czasowy w celu odszukania wizerunku twarzy. Jako odszukiwany wizerunek może być wykorzystana twarz zapisana w bazie lub dowolne rozpoznanie twarzy dokonane przez system. Co ważne, proces przeszukiwania można profilować, zmieniając wymagany stopień podobieństwa rozpoznanej twarzy do wzorca oraz ograniczając liczbę wyświetlanych wyników (fot. 3). Do każdej wyszukanej twarzy dodawana jest data i czas rejestracji, co pozwala na łatwe przejście do trybu odtwarzania.

Aby móc reagować na zagrożenia w czasie rzeczywistym, konieczny jest wybór kamer, z których



Fot. 3. Wyniki wyszukiwania osoby

chcemy otrzymywać powiadomienia alarmowe. Wśród dostępnych reakcji na rozpoznanie twarzy z wybranych baz danych jest m.in. zdalne powiadomienie wysyłane do urządzenia mobilnego i wyświetlenie informacji w formie wyskakującego okienka informacyjnego *pop-up*. Liczbę fałszywych alarmów można ograniczyć do minimum poprzez zwiększenie prawdopodobieństwa dopasowania w ustawieniach wszystkich kamer.

Interfejs sieciowy rejestratora również umożliwia dostęp do funkcji zarządzania systemem

rozpoznawania twarzy, w podobny sposób, w jaki działają funkcje z menu rejestratora. Dzięki temu mamy dostęp do statystyk dotyczących działania funkcji rozpoznania twarzy. Dane dotyczące liczby rozpoznań z podziałem na grupy są prezentowane w postaci słupków na wykresie. Wykres kołowy przedstawia dane dotyczące procentowego udziału grup, do których zakwalifikowano rozpoznaną twarz.

Fot. 4. Scenariusze powiadamiania

Również aplikacja mobilna SuperLive Plus działająca w systemach operacyjnych Android oraz iOS może odtąd służyć do wszechstronnego zarządzania rozpoznawaniem twarzy. Po uruchomieniu serwera Push w rejestratorze możliwe jest przekazywanie informacji bezpośrednio do tej aplikacji. Służy ona również do modyfikowania i uzupełniania baz twarzy.

Szczególnie wartościową funkcją jest śledzenie wybranej osoby przemieszczającej się między poszczególnymi kamerami po określeniu przedziałów czasowych jej wykrywania. Pozwala to na analizę przemieszczania się danej osoby między poszczególnymi strefami kamerowymi w obiekcie i bezpośrednie przejście do trybu odtwarzania.

Fot. 6. Śledzenie przemieszczania się osoby między polami widzenia kamer i bezpośrednie przejście do trybu odtwarzania

Fot. 5. Dodawanie nowych osób w aplikacji mobilnej w urządzeniu z systemem Android oraz przeszukiwanie bazy danych

Proces integracji różnorodnych funkcji w wizyjnych systemach dozorowych przebiega niezwykle dynamicznie. Dotyczy to zarówno funkcji rozpoznawania twarzy, jak i innych zaawansowanych funkcji analizy treści obrazu. Jest to związane z wykładniczym wzrostem mocy obliczeniowych procesorów stosowanych w kamerach i tworzeniem coraz doskonalszych algorytmów interpretowania oraz uczenia się, tak jak czyni to mózg człowieka. Na pewno w niedalekiej przyszłości zaowocuje to kolejnymi artykułami poświęconymi funkcjom, które pozwalają na efektywne sprawowanie nadzoru przy minimalnym udziale człowieka.

Patryk Gańko
AAT HOLDING

AI dla każdego
Część 2

Piotr Rogalewski

W pierwszej części przedstawione zostały podstawowe pojęcia i zagadnienia mające związek ze sztuczną inteligencją. Przytoczyłem też kilka ciekawych faktów historycznych. W niniejszej części opiszę kilka konkretnych rozwiązań leżących u podstaw sztucznej inteligencji

Po co nam sztuczna inteligencja?

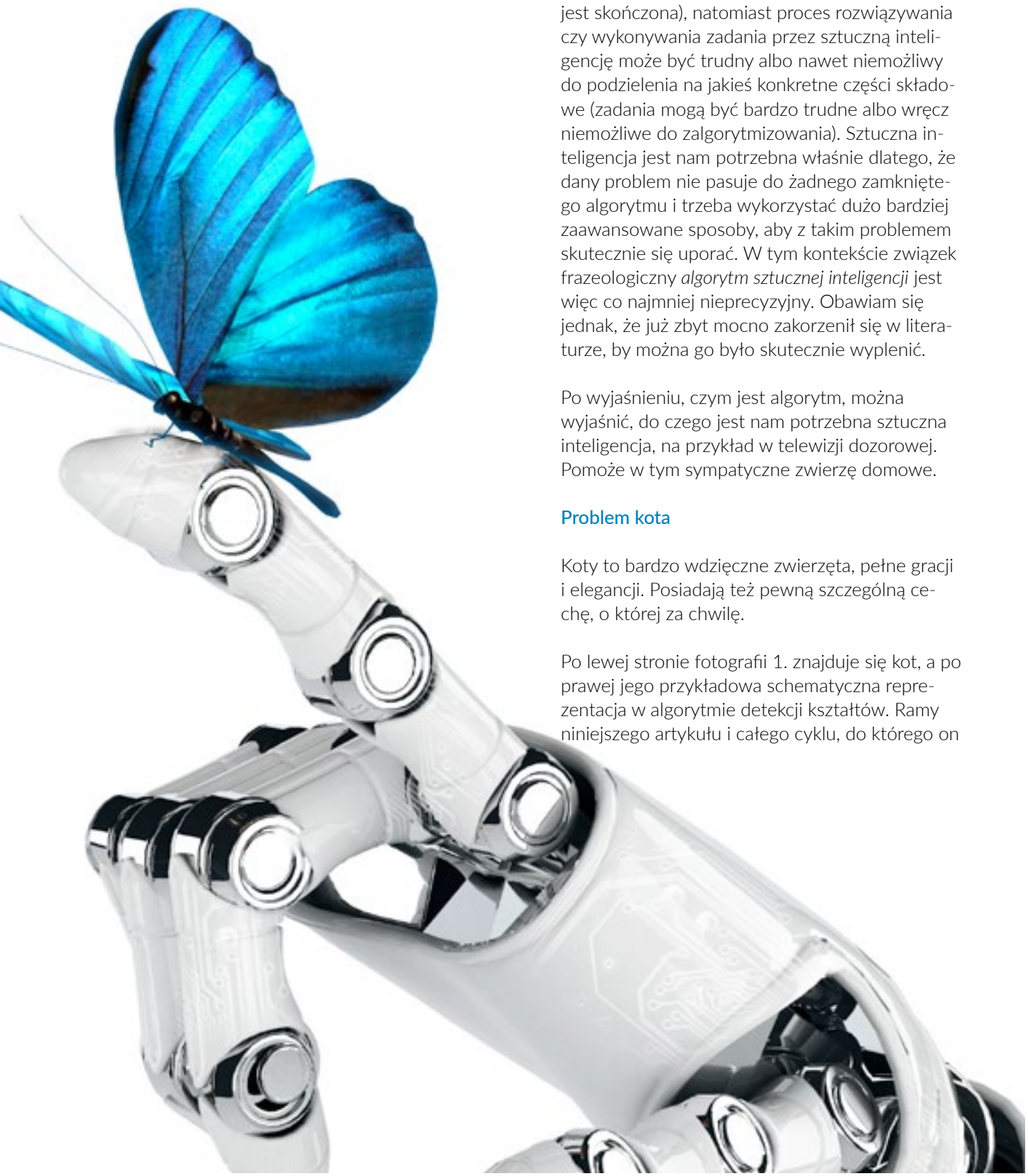
Dlaczego tak zaawansowana i skomplikowana zdobycz techniki przebojem wdziera się do naszego codziennego życia? Po części dlatego, że jako ludzie w naturalny sposób dążymy do kształtowania otaczającego nas świata w sposób, który ułatwia nam codzienne życie. W dzisiejszych czasach bardzo pomaga w tym zaawansowana technika. Wydajemy polecenia głosowe naszym telefonom, a te odpowiadają głosowymi wskazówkami nawigacyjnymi, czytają na głos wiadomości tekstowe lub podają aktualną prognozę pogody. Gdy szukamy w sieci pobliskiej restauracji, oprócz wskazówek dotyczących jej lokalizacji uzyskujemy wiele dodatkowych informacji, np. aktualne menu, listę najczęściej wybieranych dań, przedstawione opinie gości, informacje dotyczące godzin otwarcia i promocji, numer telefonu i adres poczty elektronicznej.

Gdy skierujemy aparat fotograficzny na grono znajomych, urządzenie może samo zrobić zdjęcie w momencie, gdy na twarzach fotografowanych osób pojawi się uśmiech. Gdy podczas jazdy autem wyposażonym w aktywny system bezpieczeństwa zbliżymy się zbyt szybko do pojazdu znajdującego się przed nami, zostaniemy ostrzeżeni sygnałem dźwiękowym i świetlnym, a jeśli nie zareagujemy w porę, auto rozpocznie automatycznie hamowanie awaryjne.

To kilka przykładów wykorzystania inteligencji maszyn w naszym życiu codziennym. Najważniejszym powodem, dla którego systemy sztucznej inteligencji stały się tak ważne, jest fakt, że potrafią zrobić to, co do tej pory było albo zupełnie nieosiągalne dla tradycyjnych rozwiązań informatycznych albo funkcjonowało znacznie gorzej. Do tego wątku powrócę dalej w tym artykule. Najpierw jednak warto zapoznać się z pojęciem algorytmu, które jest jednym z fundamentów informatyki.

Co to jest algorytm?

Słowo *algorytm* pochodzi od słowa *Algorismus* – łacińskiej wersji nazwiska *Al-Chuwarizmi*, arabskiego matematyka żyjącego w IX w[I]. Początkowo termin ten oznaczał sposób wykonywania działań arytmetycznych, ale po pracach Alana Turinga (zob. *AI dla każdego*, część 1, „Zabezpieczenia" nr 1/2019) i wraz z narodzinami informatyki stał się on jednym z podstawowych pojęć w tej dziedzinie. Obecnie algorytm najprościej można zdefiniować jako przepis na wykonanie czegoś. Innymi słowy jest to szereg czynności elementarnych, które należy wykonać, aby doprowadzić do rozwiązania określonego zadania[I]. Możemy więc mówić o algorytmie wykrywania twarzy czy sterowania robotem, ale takie codziennie czynności jak pieczenie ciasta, jazda samochodem czy rozmowa telefoniczna także są doskonałymi przykładami algorytmów.



Bardzo często można spotkać się z określeniem „algorytm AI" czy „algorytm sztucznej inteligencji". Nie jest to całkowicie poprawne, gdyż sama definicja algorytmu opisuje go jako sposób na wykonanie czegoś w kolejnych krokach (których liczba jest skończona), natomiast proces rozwiązywania czy wykonywania zadania przez sztuczną inteligencję może być trudny albo nawet niemożliwy do podzielenia na jakieś konkretne części składowe (zadania mogą być bardzo trudne albo wręcz niemożliwe do zalgorytmizowania). Sztuczna inteligencja jest nam potrzebna właśnie dlatego, że dany problem nie pasuje do żadnego zamkniętego algorytmu i trzeba wykorzystać dużo bardziej zaawansowane sposoby, aby z takim problemem skutecznie się uporać. W tym kontekście związek frazeologiczny *algorytm sztucznej inteligencji* jest więc co najmniej nieprecyzyjny. Obawiam się jednak, że już zbyt mocno zakorzenił się w literaturze, by można go było skutecznie wyplenić.

Po wyjaśnieniu, czym jest algorytm, można wyjaśnić, do czego jest nam potrzebna sztuczna inteligencja, na przykład w telewizji dozorowej. Pomoże w tym sympatyczne zwierzę domowe.

Problem kota

Koty to bardzo wdzięczne zwierzęta, pełne gracji i elegancji. Posiadają też pewną szczególną cechę, o której za chwilę.

Po lewej stronie fotografii 1. znajduje się kot, a po prawej jego przykładowa schematyczna reprezentacja w algorytmie detekcji kształtów. Ramy niniejszego artykułu i całego cyklu, do którego on

należy, nie pozwalają na szczegółowe opisanie działania tego typu algorytmów. Zainteresowanym zgłębieniem zagadnienia polecam np. opracowania dotyczące transformaty Hougha i detekcji linii w układzie biegunowym[II]. Dla nas istotny jest fakt, że jest to standardowy algorytm detekcji kształtów uzupełniony o mechanizm kontekstowy, nie bazujący na sztucznej inteligencji. Algorytm „widzi" okrągłą głowę, trójkątne, spiczaste uszy, podłużny tułów, cienkie, podłużne łapki i ogon. Mechanizm kontekstowy próbuje określić na podstawie wzajemnego położenia poszczególnych figur geometrycznych, czym jest dany zbiór

Fot. 1. Kot i jego schematyczna reprezentacja w standardowym algorytmie rozpoznawania kształtów. Fot.: K. Bogusz (źródło: https://pl.wikipedia.org/wiki/Kot_domowy#/media/File:Felis_catus-cat_on_snow.jpg), graf.: P. Rogalewski

kształtów, czyli czym jest w istocie obserwowany obiekt. Problem pojawia się w momencie, gdy kot wykorzysta swoją szczególną cechę, a mianowicie elastyczność ciała umożliwiającą przyjmowanie bardzo różnych pozycji.

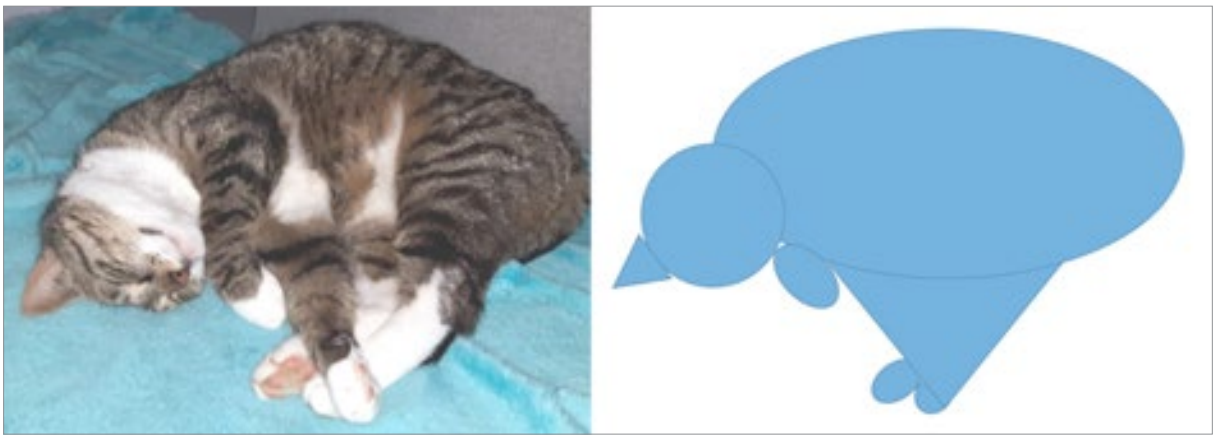
Standardowy algorytm w takiej sytuacji pogubi się całkowicie, gdyż mechanizm kontekstowy nie wykrywa, że przemieszczone w nietypowe miejsca albo nawet brakujące trójkąty, okręgi i elipsy to nadal części tego samego obiektu. W celu ustalenia, że to wciąż jest kot, będzie potrzeba znacznie więcej. To właśnie doskonałe pole do działania dla sztucznej inteligencji, która potrafi uporać się z takim zadaniem. Ale jak to robi? Skąd taki system wie, że śpiący kot to nadal kot? Odpowiedź jest prosta: bo się tego nauczył, a właściwie, ściślej rzecz ujmując, został tego nauczony. „Pokazano" mu tysiące fotografii kotów w bardzo wielu pozycjach, o różnych kolorach, różnych ras, wielkości itd. Innymi słowy system został wytrenowany do wyszukiwania kotów na obrazie. To oczywiście tylko przykład, ale w telewizji dozorowej standardowe algorytmy detekcji kształtów i analizy ruchu już dziś zaczynają oddawać pole rozwiązaniom z dziedziny sztucznej inteligencji. Oto kilka przykładów:

- poruszające się na wietrze gałęzie nad płotem będą ignorowane w odróżnieniu od człowieka przechodzącego przez ten płot;
- zwierzęta wchodzące na chroniony teren nie będą wyzwalały alarmu w odróżnieniu od osób lub pojazdów;
- w zarejestrowanym materiale zostaną odnalezione wszystkie auta określonego koloru i podanej marki, a nawet określonego modelu;
- w zarejestrowanym materiale zostaną odnalezione wszystkie osoby jadące pojazdami jednośladowymi.

Te przykładowe systemy zostały wcześniej nauczone tego, czego powinny szukać, na jakie cechy obiektów i ich zachowań zwracać uwagę, a które pomijać. Rozwiązania tego typu już istnieją i działają, a kilku czołowych producentów systemów telewizji dozorowej ma je w swojej ofercie.

AI a *big data*

Kolejne części niniejszego cyklu artykułów poświęcę w większości różnym metodom uczenia się przez maszyny lub systemy (ang. *machine learning*), często nazywanego w języku polskim uczeniem maszynowym (to określenie już zdążyło się upowszechnić), gdyż jest to fundamentalny element sztucznej inteligencji. Zacznę jednak od uporządkowania kategorii procesów w ramach sztucznej inteligencji.



Fot. 2. Śpiącego kota kompletnie nie interesuje problem, jaki stwarza on algorytmowi detekcji kształtów. Fot. i graf.: P. Rogalewski

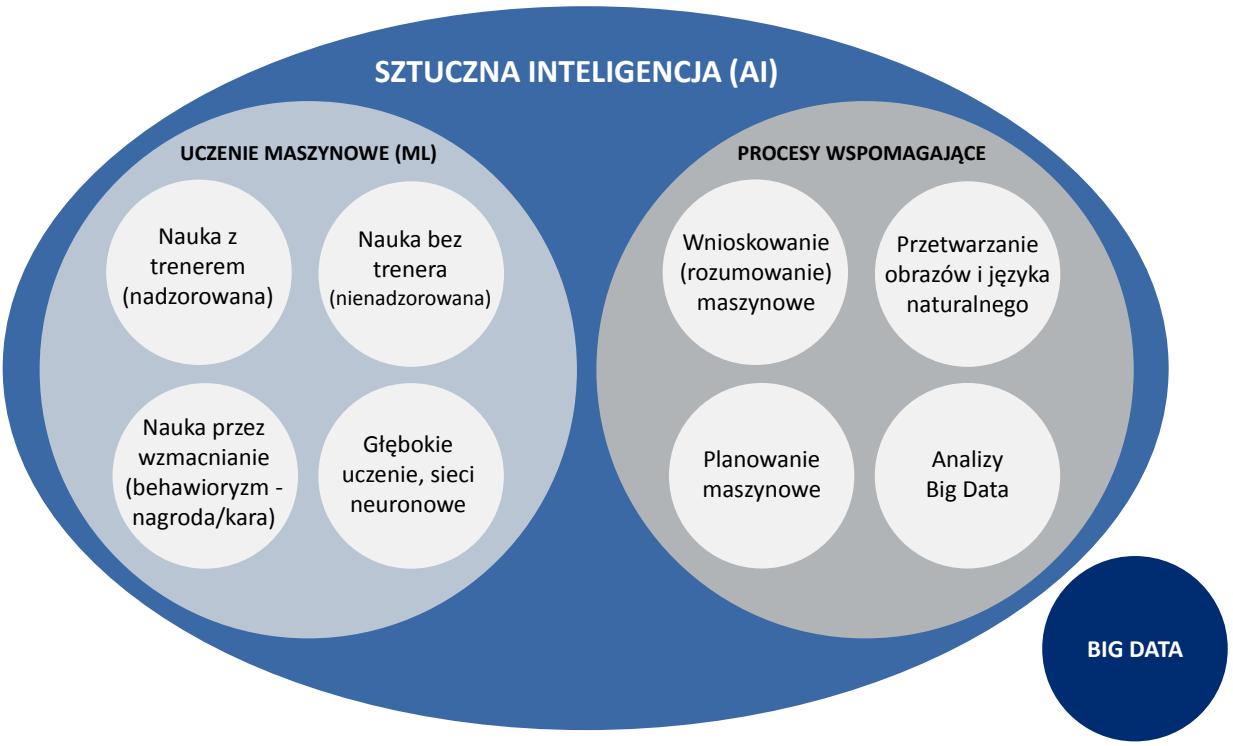
Sztuczna inteligencja nie mogłaby istnieć bez bardzo dużych zbiorów danych (ang. *big data*)[III] – tak dużych, że przetwarzanie ich tradycyjnymi metodami jest znacznie trudniejsze niż samo gromadzenie danych i często nie jest możliwe. Obecnie napisanie aplikacji posługującej się sztuczną inteligencją wcale nie wykracza poza możliwości małego zespołu średniej klasy programistów. Co więc powoduje, że prym w tej dziedzinie wiodą giganci, tacy jak Google, Microsoft czy Facebook? Wbrew pozorom zaplecze finansowe niekoniecznie jest tu na pierwszym miejscu. Kluczem są właśnie ogromne zbiory danych, którymi można „karmić" systemy wykorzystujące sztuczną inteligencję i je skutecznie trenować. Proponuję wpisanie w wyszukiwarce internetowej słowa *kot*. Liczba wyników, podawana w górnej części strony daje pojęcie o ogromie zbioru zgromadzonych danych – w tym przypadku jest to liczba użyć słowa *kot* w najrozmaitszych kontekstach. To doskonały przykład użycia *big data*.

W ramach sztucznej inteligencji możemy wyróżnić dwie główne kategorie procesów: uczenie się przez maszyny lub systemy (*machine learning*), po polsku nazywane uczeniem maszynowym, oraz procesy wspomagające. Ten podział nie jest dokładny, bo bardzo często procesy z obu kategorii wzajemnie się przenikają i uzupełniają, jednak zastosuję go w celu uporządkowania różnych pojęć. Ogólnie rzecz ujmując, procesy wspomagające to ta część sztucznej inteligencji, która nie zajmuje się bezpośrednio uczeniem się, tylko przygotowaniem zbiorów danych do niego potrzebnych, czyli materiałów do nauki oraz opracowaniem i wykorzystaniem wyników uczenia się. Do elementów z tej kategorii wrócę w kolejnych częściach cyklu, by teraz skupić się na *machine learning*.

Nauka czyni mistrza

Uczenie się przez maszyny lub systemy (albo, inaczej mówiąc, uczenie maszynowe) umożliwia maszynom realizację zadań bez precyzyjnych instrukcji lub ich wykonania pomimo braku części danych koniecznych do wykonania takich zadań[IV]. Wykorzystując sztuczną inteligencję, maszyny same mogą zdobywać brakujące dane (wiedzę), czyli się uczyć. Uczenie maszynowe jest więc naturalną konsekwencją i wynikiem rozwoju sztucznej inteligencji. Na rys. 1. widoczne są cztery kategorie odpowiadające różnym metodykom uczenia się:

1. Nauka z trenerem (nadzorowana). Zakłada udział nadzoru w procesie uczenia się i opiera się na porównywaniu nowych danych z dostępnymi, znajdującymi się w pamięci, przykładowymi („treningowymi") parami informacji, z których jedna jest „wejściowa", a druga „wyjściowa" (dostępne dane mogą być w zasobach określanych mianem *big data*). Innymi słowy, system – „widząc", jak dane dostarczone przez trenera wpływają na wynik „na wyjściu" – będzie starał się przewidzieć, jaki wynik „na wyjściu" dadzą nowe dane wejściowe, których wcześniej nie „widział".
2. Nauka bez trenera (nienadzorowana). W tym przypadku system nie otrzymuje z zewnątrz żadnych wskazówek dotyczących relacji między danymi wejściowymi i wyjściowymi. Będzie starał się wyciągać wnioski samodzielnie, np. na podstawie powtarzalności i regularności w danych wejściowych, grupowania ich w zbiory, sortowania itp.
3. Nauka przez wzmacnianie. Po podjęciu decyzji na podstawie dostępnych danych



Rys. 1. Uczenie maszynowe i procesy wspomagające sztuczną inteligencję. Graf.: P. Rogalewski

wejściowych system ulega tzw. wzmocnieniu (wzmocnieniu pozytywnemu), jeżeli decyzja okazała się słuszna, albo tzw. wzmocnieniu negatywnemu po podjęciu niesłusznej decyzji, co jest mechanizmem opisanym w psychologii behawioralnej (wzmocnienie pozytywne jest nagrodą, a wzmocnienie negatywne karą). Wzmocnienie pozytywne jest w tym przypadku silnym, a wzmocnienie negatywne słabym sygnałem odbieranym przez system

4. Głębokie uczenie się. Jest to metoda polegająca na wielopoziomowej analizie danych wejściowych, na przechodzeniu od ogółu do szczegółu. Metoda ta, obok automatycznego uczenia się przez system (ang. *automatic machine learning*), jest obecnie najbardziej zaawansowaną i najbardziej skomplikowaną techniką wspierającą systemy wykorzystujące sztuczną inteligencję.

W kolejnej części skoncentruję się na szczegółach technik uczenia maszynowego i opiszę działanie podstawowego elementu sieci neuronowych – sztucznego neuronu.

Piotr Rogalewski

Przypisy

[I] Lidia Drabik, Elżbieta Sobol, *Słownik języka polskiego PWN*, Wydawnictwo Naukowe PWN, Warszawa 2018.

[II] R. O. Duda, P. E. Hart, *Use of the Hough Transformation to Detect Lines and Curves in Pictures*, (w:) „Association for Computing Machinery", vol. 15, styczeń 1972.

[III] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, Houghton Mifflin Harcourt, Boston 2013.

[IV] T. Mitchell, *Machine Learning*, McGraw-Hill, Nowy Jork 1997.

SPRAWDŹ
JAK ZMIENIAMY
SIĘ DLA CIEBIE

NOWA STRONA INTERNETOWA

OPROGRAMOWANIA
NMS

www.nms.aat.pl

www.nms.aat.pl

Mikrolokalizacja i beacony

wsparcie oraz konsolidacja procesów bezpieczeństwa

Dominik Piepka

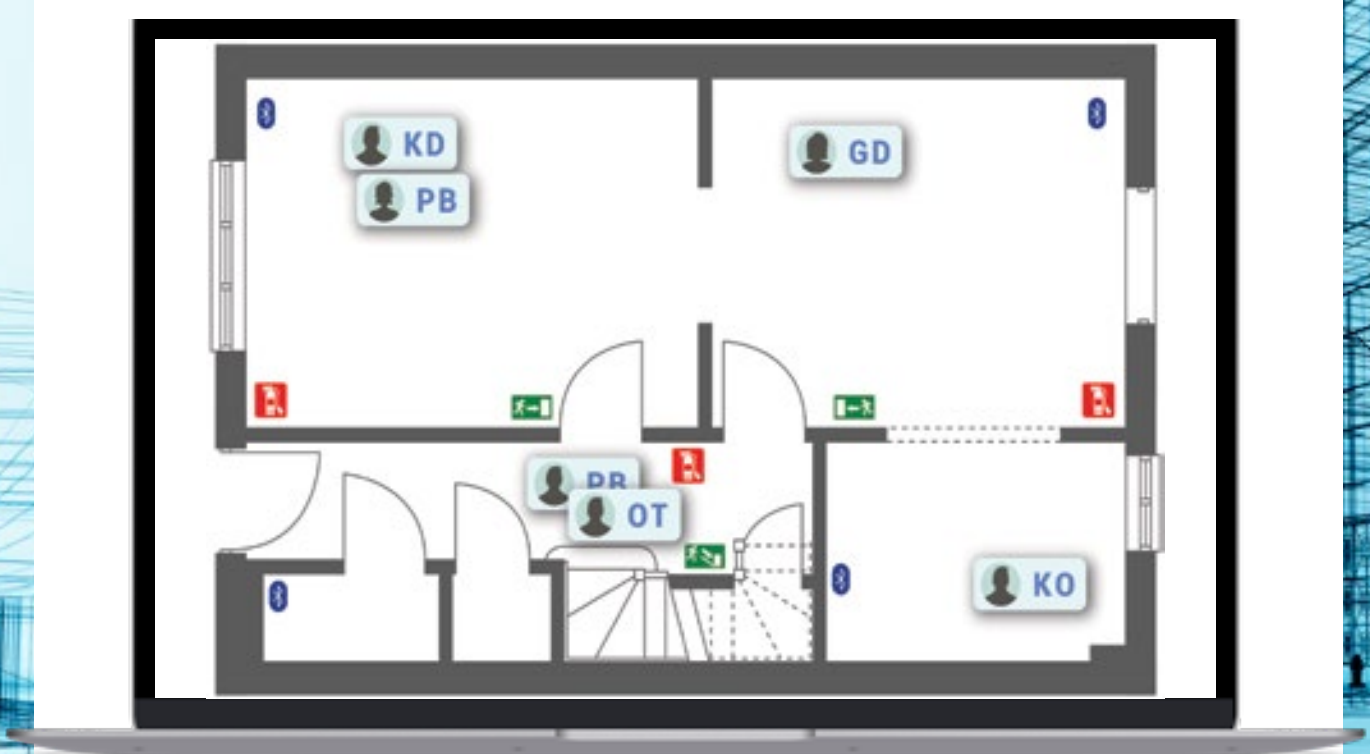
Powszechnie stosowane systemy GPS przyzwyczaiły nas do precyzyjnej lokalizacji obiektów w przestrzeni otwartej. Niestety wewnątrz budynków nawigacja satelitarna nie działa, między innymi dlatego, że sygnał generowany przez satelity GPS jest za słaby, żeby przeniknąć przez ściany czy sufity. Obiekty znajdujące się w pomieszczeniach zamkniętych, również w budynkach wielopiętrowych, można skutecznie lokalizować z wykorzystaniem standardu komunikacji bezprzewodowej Bluetooth Low Energy (BLE) zwanego też Bluetoothem Smart

Główne zalety standardu BLE, takie jak mały pobór mocy, szybki dostęp do danych oraz zwiększony zasięg działania (moduły radiowe BLE są powszechnie stosowane w smartfonach oraz wykorzystywane przez aplikacje mobilne), umożliwiły zbudowanie nowego rodzaju urządzeń pracujących długo i zasilanych z małych baterii. Przykładem takich urządzeń są beacony – niewielkie nadajniki z własnym zasilaniem, które cyklicznie wysyłają sygnały przenoszące pakiety danych (np. dane telemetryczne dotyczące czasu, temperatury, ruchu), możliwe do rozpoznania przez urządzenia odbiorcze, np. smartfony lub inne odbiorniki BLE znajdujące się w najbliższym otoczeniu beaconów. Beacony nie mogą być efektywnie wykorzystywane bez odpowiedniego oprogramowania, np. w postaci aplikacji mobilnych, ale dzięki niskiemu zużyciu energii mogą działać na jednej baterii, bez ładowania, nawet przez kilka lat. Co ważne,

Fot. 1. Card Tag CT18-3. Kontakt.io

beacony BLE mogą przybrać różne formy, np. małego taga montowanego na ścianie lub karty zbliżeniowej (fot. 1).

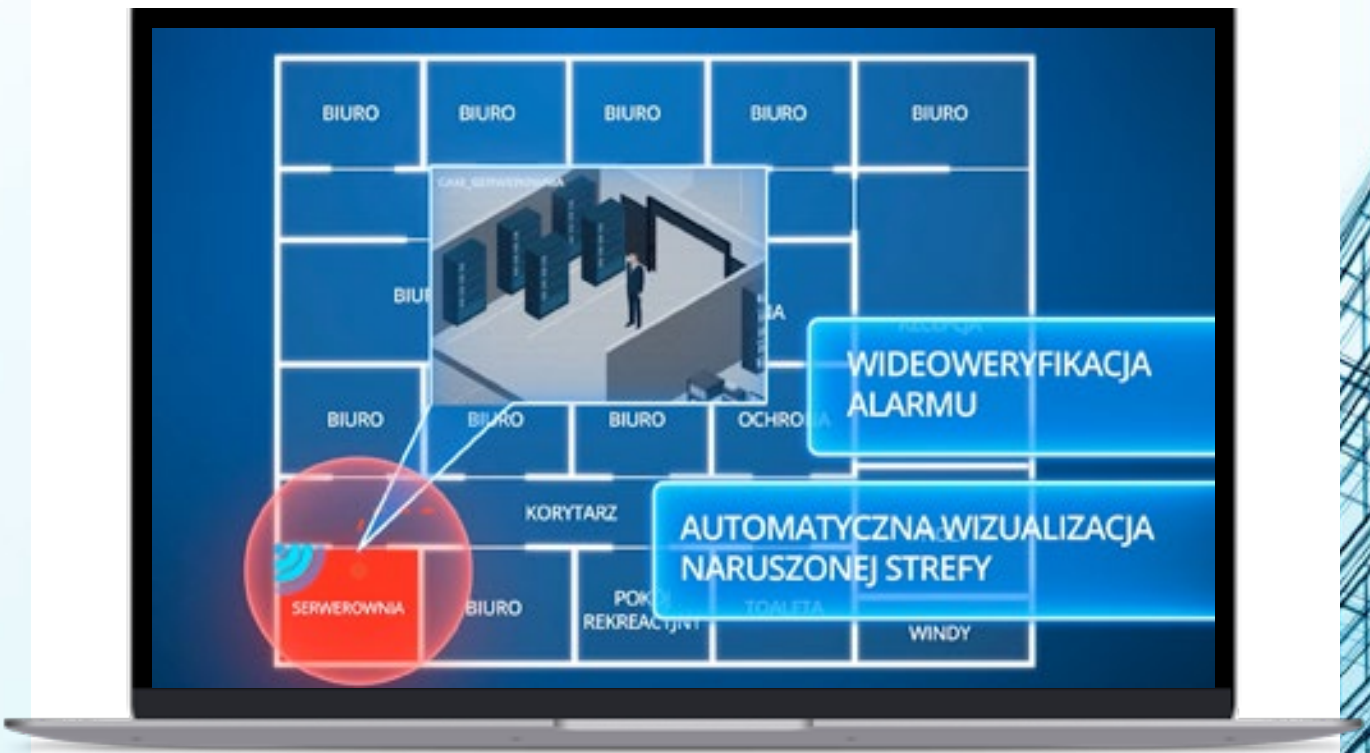
W celu precyzyjnego ustalenia położenia obiektu w przestrzeni, np. lokalizacji osoby w pomieszczeniu, opracowano różne metody i algorytmy analizy sygnałów odbieranych od beaconów BLE, m.in. pozwalające ustalić odległość pomiędzy obiektem a beaconem BLE czy trasę przemieszczania się obiektu. Jeżeli na określonym obszarze wewnątrz budynku, np. na korytarzu i w pomieszczeniach połączonych z korytarzem, zainstalujemy odbiorniki BLE, a osoby poruszające się po takiej strefie będą wyposażone w identyfikatory w postaci beaconów, to – korzystając z odpowiedniego oprogramowania – będzie można wizualizować położenie tych osób na rzutach pięter budynku. Taki sposób określania położenia przedmiotów lub osób nazywamy *mikrolokalizacją*. Poruszanie się obiektów można kontrolować na bieżąco na ekranie komputera bądź urządzenia mobilnego (rys. 1). Beacony są wykorzystywane najczęściej w marketingu i handlu internetowym, np. w celu przesyłania klientom korzystającym z odpowiedniej aplikacji sklepowej kontekstowych informacji o produktach. Urządzenia te oraz mikrolokalizacja mogą jednak być wykorzystane także w procesach związanych z ochroną osób i mienia. W tym miejscu warto zwrócić uwagę na funkcje systemu Smart Indoor Location związane z bezpieczeństwem (rys. 2.) Korzystając z identyfikatorów beaconowych w formie karty zbliżeniowej (na fot. 1 przedstawiona jest karta kompatybilna z większością czytników kontroli dostępu) oraz tagów beaconowych współpracujących z modułami odbiorczymi BLE, które instaluje się w wybranych pomieszczeniach wewnątrz budynku, można uzyskać szereg dodatkowych funkcji. Na przykład



Rys. 1. Lokalizacja osób poruszających się wewnątrz budynku przez Smart Indoor Location

Rys. 2. Funkcje systemu Smart Indoor Location

można precyzyjnie lokalizować gości wchodzących do budynku, dostawców, pracowników oraz monitorować przemieszczanie się tych osób po budynku, nadawać uprawnienia do poruszania się wyłącznie po wyznaczonych strefach (np. tylko na konkretnym piętrze i w konkretnym pomieszczeniu) oraz być alarmowanym w przypadku wejścia tych osób do stref zabronionych. Możliwe jest też automatyczne wygenerowanie alarmu po wykryciu czyjegoś upadku lub pozostawania danej osoby w bezruchu. System umożliwia rejestrowanie czasu przebywania osób w konkretnym pomieszczeniu, pokazywanie zmiany położenia obiektu (np. jeżeli tagiem beaconowym oznakujemy laptop i zostanie on przeniesiony do innego pomieszczenia), a w przypadku integracji z lokalnym system CCTV także wizyjną weryfikację w strefach objętych polem widzenia kamer (rys. 3). Bardzo ciekawą funkcją jest alarmowanie o zagrożeniu lub złym samopoczuciu osób



Rys. 3. Wizualizacja naruszonej strefy dzięki systemowi Smart Indoor Location

Wystarczy wcisnąć wbudowany w kartę przycisk (fot. 1), a beacon wyśle ostrzeżenia do systemu, który przekaże informację w określony wcześniej sposób, np. wygeneruje ostrzeżenie dla pracowników ochrony i wyświetli dokładną lokalizację osoby wzywającej pomocy na planie budynku. To wszystko odbywa się w czasie rzeczywistym. Innym przykładem zastosowania beaconów BLE w dziedzinie bezpieczeństwa, a także smartfonów i mobilnych aplikacji do kontroli dostępu, jest umożliwienie klientom banku (którzy zdecydowali się na korzystanie z odpowiedniej aplikacji) wejścia po godzinach pracy do stref ATM w wybranych placówkach. Wejście jest otwierane za pomocą smartfona i nie ma potrzeby wyjmowania w tym celu karty. Powyższe rozwiązanie ma dawać klientom banku poczucie bezpieczeństwa, ponieważ nie muszą wyciągać portfela czy karty bankomatowej w niezabezpieczonym środowisku.

Systemy i aplikacje wykorzystujące beacony BLE pod różną postacią mogą pełnić funkcje, które konsolidują i wspierają procesy kontroli dostępu, ochrony mienia, rejestracji czasu pracy oraz ochrony ludzi. Instalacja przewodowej lub bezprzewodowej infrastruktury, wymaganej do prawidłowego działania systemów, w których wykorzystywane są beacony BLE, jest prosta. Oprogramowanie monitorujące może być instalowane na serwerach klienta bądź w chmurze dostawcy aplikacji. Możliwa jest integracja z innymi systemami zabezpieczeń.

Dominik Piepka

Rzeczoznawca Polskiej Izby Ochrony,
Certyfikowany Manager Bezpieczeństwa
i Ochrony
dpiepka.rzeczoznawca@piooim.pl

POLON-ALFA

PROJEKTUJEMY zgodnie ze sztuką

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A.

85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

Projekt dobry, projekt zły?
Jak i po co oceniać projekty?

Każdej organizacji zależy na tym, żeby oferowane przez nich produkty i usługi były atrakcyjne i niosły wartość dla klientów/odbiorców. Jednak klienci wciąż generują nowe potrzeby i oczekiwania a postęp technologiczny jest niezwykle dynamiczny. Czynniki te sprawiają, że organizacja ma niewiele czasu, żeby uatrakcyjniać i dostosowywać swoją ofertę do potrzeb rynku. Stąd presja na ciągłą poprawę skuteczności i efektywności realizowanych przedsięwzięć i projektów.

A projekty są wszędzie. Projektem jest już nie tylko budowa mostu czy hali produkcyjnej. Projektem jest wdrożenie nowego rozwiązania do systemów zabezpieczeń u klienta, wdrożenie systemu IT ale również zorganizowanie unikatowego wydarzenia czy wprowadzenie usprawnienia w firmie.

Jak zatem oceniać praktyki projektowe w organizacji i gdzie szukać potencjału do dalszego doskonalenia? Jak weryfikować czy projekty są dobrze realizowane i zarządzane przy tak różnych obecnie rodzajach projektów i indywidualnym podejściu firm i organizacji do zarządzania projektami? Jak w samym procesie zarządzania projektami zidentyfikować mocne strony projektu i możliwości usprawnień? Czy istnieje do tego jakieś uniwersalne narzędzie?

Project Excellence Model

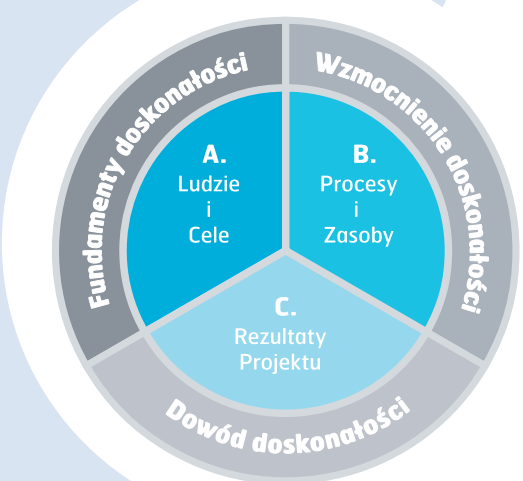
International Project Management Association – organizacja non-profit działająca na rzecz rozwoju dziedziny project management w Polsce i na świecie, opracowała model Project Excellence.
Zalety modelu:

- umożliwia kompleksową ewaluację zarówno samego procesu zarządzania danym projektem, jak i jego szeroko rozumianych rezultatów.
- wyjaśnia jak doskonalić zarządzanie projektami kluczowymi dla realizacji strategii organizacji.
- może być stosowany niezależnie od podejścia do realizacji projektu
- nie narzuca żadnego konkretnego podejścia w zakresie dekompozycji, organizacji i planowania projektu
- nie sugeruje żadnych konkretnych technik ani narzędzi zarządzania projektem.
- kładzie nacisk na świadome wykorzystywanie najbardziej skutecznych metod i formuł zarządzania, pozwalających osiągnąć założone rezultaty i umożliwiających ciągłe doskonalenie.

Model jest na tyle uniwersalny, że nie ma znaczenia branża, wielkość ocenianego projektu, rodzaj projektu, przyjęta metodyka zarządzania projektem czy źródła finansowania.

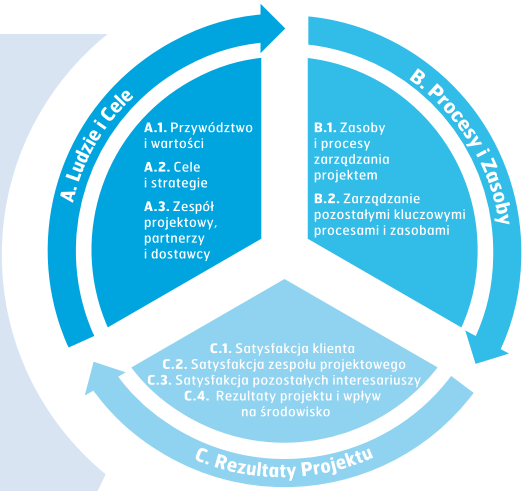
W modelu analizowane są następujące kryteria:

1. Ludzie i Cele - obszar ten uznaje się za fundament doskonałości w zarządzaniu projektami. Właściwi ludzie, kierowani i wspierani przez doskonałych liderów oraz dzielący z nimi wspólną wizję sukcesu, mają kluczowe znaczenie dla ciągłego doskonalenia w projekcie i pozwalają mu wykroczyć poza granice znanych standardów.
2. Procesy i Zasoby - obszar ten obejmuje praktyki niezbędne do wzmacniania doskonałości przez czytelne i skuteczne procesy oraz adekwatne zasoby wykorzystywane w sprawny i zrównoważony sposób. Stanowi on także podstawę do zabezpieczenia rezultatów wynikających z innowacyjności, czyniąc je solidnym punktem wyjścia dla kolejnych udoskonaleń.
3. Rezultaty Projektu - podejście do zarządzania projektem może zostać uznane za doskonałe, wyłącznie jeżeli prowadzi do wyróżniających się, zrównoważonych rezultatów dla wszystkich kluczowych interesariuszy. Obszar ten stanowi dopełnienie pierwszych dwóch, zapewniając niezbędny dowód osiągnięcia doskonałych rezultatów zgodnych z oczekiwaniami interesariuszy projektu.



Rys. 1. Interpretacja obszarów modelu

Każdy z wymienionych obszarów jest podzielony na bardziej szczegółowe podkryteria. A to pozwala na dokonanie wnikliwej analizy mocnych stron projektu i obszarów do doskonalenia.



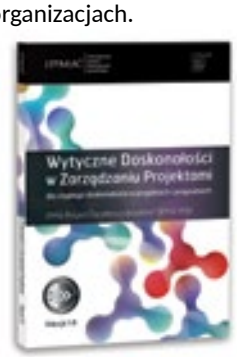
Rys. 2. Kryteria IPMA PEM

Cechą unikatową modelu jest wskazanie obszaru „Ludzie i cele" jako fundamentu doskonałości. To liderzy określają odpowiednie wartości i kierują się nimi. Wg założeń modelu to „Liderzy angażują kluczowych interesariuszy w określanie celów projektu i opracowywanie strategii ich realizacji. Tworzą oni efektywne zespoły i angażują właściwych partnerów i dostawców, umożliwiając skuteczną realizację projektów."

Model, o którym mowa został szczegółowo opisany w wydanym przez IPMA standardzie: „Wytyczne Doskonałości w Zarządzaniu Projektami – dla ciągłego doskonalenia w projektach i programach." W firmach i organizacjach jest wykorzystywany przy:

- ocenie projektów i programów
- benchmarkingu projektów i programów
- odkrywaniu obszarów doskonałego zarządzania projektami i portfelami
- uznaniu doskonałego przywództwa

Z modelu korzystają głównie kierownicy projektów, programów i portfeli oraz biur zarządzania projektami, a także kierownictwo wyższych szczebli w firmach i organizacjach.



Jako organizacja non-profit, IPMA Polska promuje standardy i dobre praktyki w zarządzaniu projektami, stąd udostępnia Członkom Stowarzyszenia bezpłatną wersję elektroniczną Project Excellence Baseline.

Fot. 1. "Wytyczne Doskonałości w Zarządzaniu Projektami – dla ciągłego doskonalenia w projektach i programach." International Project Management Association

Wioletta Kastrau IPMA Polska
wioletta.kastrau@ipma.pl
Tel. 600509129

Zagrożenia podczas korzystania z komputera i Internetu

Andrzej Walczyk

Obecnie niemal wszyscy mieszkańcy Ziemi korzystają z Internetu. Użycie słowa niemal jest jak najbardziej uzasadnione, gdyż jedynie nieliczna grupa ludzi tego nie robi. Nawet małych dzieci nie można wykluczyć z tego grona, gdyż te zaczynają przeglądać obrazki w smartfonach rodziców, zanim nauczą się mówić. Śmiało można stwierdzić, że korzystanie z globalnej sieci stało się masowe

Trudno nie docenić dobrodziejstw wynikających z masowego wykorzystania Internetu. Oferta przeznaczona dla osób prywatnych jest bardzo szeroka i nadal się poszerza. Korzystając z Internetu, robimy zakupy, przeprowadzamy operacje bankowe, płacimy podatki, uczymy się i studiujemy, czytamy gazety, oglądamy filmy, prowadzimy korespondencję, nawiązujemy znajomości, bawimy się, udostępniamy innym wyniki swojej pracy, czyli robimy to wszystko, co zaledwie kilkadziesiąt lat temu wymagało naszej fizycznej obecności w różnych miejscach.

Wielu czynności nie możemy wykonać inaczej niż przez Internet. Nasze uzależnienie od Internetu jest coraz silniejsze, tymczasem zbyt mało ludzi ma świadomość wynikających z tego zagrożeń. Czy jesteśmy bezpieczni, przeprowadzając operacje na połączonym z Internetem domowym komputerze, przenośnym tablecie lub smartfonie? Płacąc za zakupy w sklepie internetowym, podajemy w niektórych przypadkach wszystkie dane z karty kredytowej. Na tej podstawie sprzedawca obciąża konto bankowe kupującego. Dowolna osoba, która przechwyci transmisję i wejdzie

w posiadanie tych danych, będzie mogła dokonywać zakupów na koszt właściciela karty. Takie jest ryzyko, jednak miliardy ludzi nie przestaną korzystać z możliwości robienia zakupów przez Internet. Jak zapewnić sobie bezpieczeństwo?

Faktyczne bezpieczeństwo i poczucie bezpieczeństwa to dwie różne rzeczy. Większość użytkowników komputerów w ogóle nie zdaje sobie sprawy z czyhających zagrożeń. Przestępczość, zarówno pospolita, jak i zorganizowana, przeniosła się do Internetu, więc nie zawsze jesteśmy bezpieczni nawet we własnych domach. Do Internetu przenieśli się także oszuści, którzy grają na ludzkich emocjach, stwarzają prowokacyjne sytuacje, liczą na spontaniczne, nieprzemyślane działania, korzystają z metod socjotechnicznych.

Pocztą elektroniczną mogą być rozsyłane na przykład informacje dotyczące dostawy towarów, które w ogóle nie były zamówione, fikcyjne oferty pracy i propozycje, które rzekomo mają umożliwić szybkie zarobienie dużych sum pieniędzy, powiadomienia o wysokich wygranych na loteriach, wezwania do zapłaty zaległych faktur. Często zdarza się, że otrzymane wiadomości przypominają takie, które dostajemy od zaufanych nadawców, np. z banku. W takiej sytuacji trudno powstrzymać się od kliknięcia jaskrawego napisu „sprawdź ofertę", choćby tylko z ciekawości. Skutek może być katastrofalny – w najlepszym przypadku instalacja złośliwego oprogramowania, w najgorszym zniszczenie wszystkich danych na dysku.

Innego rodzaju zagrożenia stwarzają hakerzy, którzy z różnych przyczyn starają się włamać do komputerów należących do osób prywatnych. Cele mogą być bardzo różne – chęć sprawdzenia swoich sił czy przejrzenia zawartości czyjegoś dysku, wykradzenie lub zniszczenie efektów czyjejś pracy, okradzenie kogoś z pieniędzy.

Ostatnio dochodzi też do ataków hakerskich powodujących zaszyfrowanie danych na dysku komputerowym. Po dokonaniu ataku haker kontaktuje się z właścicielem komputera i proponuje podanie hasła do jego własnego dysku za określoną sumę pieniędzy. Bardzo często złośliwe działania hakerów są prowadzone jedynie w celu zyskania rozgłosu, a nie dla pieniędzy. Jedyną nagrodą może być w tym przypadku informacja w prasie dotycząca czyjegoś wyczynu.

Pomysłowość oszustów internetowych jest równie wielka jak tych, którzy kiedyś działali bez wykorzystania sieci. Różnica polega na zastosowaniu innych środków technicznych. Tło psychologiczne i społeczne pozostało bez zmian. Oszuści korzystają z elementarnych przywar ludzkich, takich jak ciekawość, łatwowierność, chciwość, a także – nazwijmy to po imieniu – ze zwykłej głupoty.

Żyjąc we współczesnym świecie, nauczyliśmy się rozpoznawać występujące w nim zagrożenia i im przeciwdziałać. Człowiek wychodzący na ulicę zachowuje czujność, trzyma portfel w zamkniętej kieszeni, nie wchodzi w ciemne zaułki etc. Człowiek przemieszczający się w wysokich górach wie, że może spaść w przepaść, więc nie schodzi z wytyczonych szlaków. Niestety wielu użytkowników Internetu w ogóle nie ma poczucia zagrożenia i nie przestrzega podstawowych zasad bezpieczeństwa.

Użytkownik komputera nie musi być informatykiem, tak jak kierowca nie musi znać się na mechanice samochodowej. Obaj są użytkownikami sprzętu, który ktoś wyprodukował, a ktoś inny im sprzedał. Poczucie bezpieczeństwa może wynikać z przekonania, że zadbał o nie zarówno producent, jak i dostawca. W przypadku samochodów jest to bliskie prawdy, gdyż każdy nowy model przechodzi drobiazgowe badania i musi spełniać odpowiednie wymagania – w przeciwnym razie nie zostanie dopuszczony do ruchu. W przypadku komputerów jest inaczej.

Komputer jest urządzeniem zdolnym do wykonywania skomplikowanych działań zgodnie z programem, który zostanie do niego wprowadzony. Współczesne komputery są na tyle doskonałe, że mogą wykonywać wiele zadań jednocześnie. Wszystko jest w porządku, o ile programy zostały świadomie wprowadzone przez producenta, a później także przez użytkownika. Nikt jednak nie jest w stanie zagwarantować, że do komputera nie dostaną się jakieś inne, niepożądane programy. Porównanie do wirusowego zainfekowania żywego organizmu jest bardzo trafne.

Wirusy komputerowe są małymi programami, które mają zdolność do modyfikowania działania komputerów zgodnie z intencjami ich twórców. Sposobów na to, by wirus lub inny szkodliwy program mógł się przedostać do komputera, jest wiele. Najczęściej stanowi on fragment jakiegoś z pozoru bezpiecznego oprogramowania. Może także zostać dołączony do wiadomości wysłanej pocztą elektroniczną lub nieumyślnie pobrany z oglądanej strony WWW.

Oczywiście wirusy komputerowe nie powstają samoistnie. Są wytwarzane przez ludzi. Inwencja ich twórców bywa ogromna. Często są to wybitnie uzdolnieni programiści, którzy doskonale znają swoje rzemiosło. Trzeba jednak podkreślić, że w infekowaniu swoich, a także cudzych komputerów ważną rolę mogą odgrywać także zupełnie nieświadomi tej roli użytkownicy. Ich nieodpowiedzialne działania znacznie ułatwiają pracę hakerom i autorom złośliwego oprogramowania.

Jedną z naczelnych zasad bezpiecznego korzystania z Internetu jest stosowanie tak zwanych mocnych haseł czyli takich, które trudno odgadnąć. Mocnym hasłem jest zbiór przypadkowych znaków, który nie oznacza niczego konkretnego. Niestety mocne hasła mają to do siebie, że trudno je zapamiętać.

Drugą, równie ważną zasadą jest nieużywanie tych samych haseł w wielu aplikacjach. Jeśli nie przestrzega się tej zasady, można na przykład umożliwić komuś okradzenie konta bankowego po podaniu tego samego hasła dostępowego, które zostało użyte w celu kupienia biletów na pociąg.

Przestrzeganie tylko tych dwóch zasad wymaga od użytkownika Internetu sporej dyscypliny. Trzeba stworzyć i często zmieniać wiele haseł, co na dalszą metę może być uciążliwe i prowadzić do pomyłek. Z pomocą przychodzą programy do zarządzania hasłami, jednak technika nie wystarczy – trzeba być świadomym zagrożenia i chcieć zastosować odpowiednie zabezpieczenia.

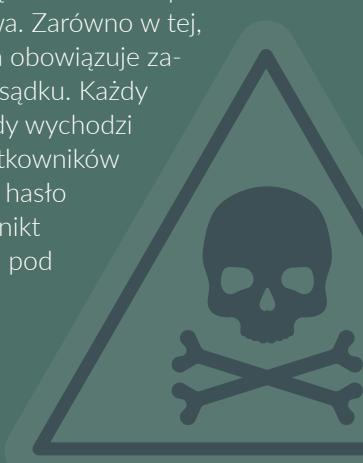
Przykładem poważnego zaniedbania jest pozostawienie fabrycznych haseł w nowo zakupionych urządzeniach. W bardzo wielu sieciach domowych pozostawione są fabryczne ustawienia rutera, co pozwala na zmianę jego konfiguracji zupełnie dowolnej osobie, która przypadkowo lub celowo pozna jego adres w sieci publicznej. Cena za popełnienie takiego błędu może być wysoka, wszystkie przesyłane dane, w tym korespondencja, niezaszyfrowane hasła i inne dane o szczególnym znaczeniu, stają się dostępne dla hakerów.

Powszechnie znane jest zalecenie, by świadomie korzystać z przeglądarki stron WWW, lecz jego spełnienie bywa trudne. Jak odróżnić stronę wolną od złośliwego oprogramowania od strony specjalnie stworzonej w celu rozsiewania takiego oprogramowania? W wielu przypadkach komputer wyświetla ostrzeżenia przed złośliwymi stronami, ale i te są ignorowane. Podczas przeprowadzania operacji finansowych konieczne jest korzystanie z połączeń szyfrowanych, ale i na to wielu użytkowników nie zwraca uwagi.

O własne bezpieczeństwo trzeba zadbać poprzez tworzenie zapasowych kopii danych dyskowych. Mało kto zdaje sobie sprawę z ogromu strat, które mogą być następstwem zwyczajnej awarii lub celowego uszkodzenia lub zaszyfrowania twardego dysku w komputerze. Żartem mówi się, że użytkownicy komputerów dzielą się na tych, którzy regularnie tworzą kopie zapasowe danych ze swoich dysków, oraz tych, którzy dopiero będą je tworzyć.

Nieprofesjonalni użytkownicy komputerów i Internetu sami przyczyniają się do obniżenia poziomu własnego bezpieczeństwa. Zarówno w tej, jak i w innych dziedzinach życia obowiązuje zasada zachowania zdrowego rozsądku. Każdy z nas zamyka drzwi na klucz, gdy wychodzi z domu, jednak tylko część użytkowników komputerów ma wprowadzone hasło do systemu operacyjnego, aby nikt nie mógł uruchomić komputera pod nieobecność właściciela.

Andrzej Walczyk



Bezpieczeństwo dzięki aplikacjom mobilnym

Michał Konarski

Od kilku lat urządzenia mobilne są w fazie swojej technicznej dojrzałości. Ich możliwości okrzepły, przestały nas już zaskakiwać nowymi funkcjami i rozwiązaniami. Wraz z osiągnięciem tej fazy rozwoju zaczęły znajdować coraz więcej profesjonalnych zastosowań

Czym są te urządzenia, bez których ciężko wyobrazić sobie sprawne funkcjonowanie w dzisiejszych czasach? W dużym uproszczeniu są to przenośne komputery wyposażone w wysokowydajne jednostki obliczeniowe, wyświetlacze i kamery o dużych możliwościach, jednostki geolokalizacyjne oraz liczne interfejsy komunikacyjne. Przybierają one postać telefonów i tabletów, które są przystosowane do wielogodzinnej autonomicznej pracy bez zasilania zewnętrznego. Tak jak w przypadku komputerów, o funkcjonalności urządzeń mobilnych decyduje oprogramowanie, które możemy na nich uruchomić – tak zwane aplikacje mobilne.

Jeszcze kilka lat temu w branży technicznej ochrony mienia panowała swego rodzaju stagnacja. Brakowało spektakularnych zmian technologicznych, które miałyby szansę zrewolucjonizować rynek. Producenci sprzętu przez wiele kolejnych lat wytwarzali urządzenia o podobnych funkcjach, zaś w sektorze usług trwała wykańczająca rynek wojna cenowa o najniższe stawki gwarantowane w umowach – często niższe od całkowitych kosztów własnych.

Na szczęście fala cyfrowej rewolucji, która porwała również tę z pozoru konserwatywną branżę, przyniosła świeży powiew. Zmiany, które dostrzegają chyba wszyscy, dotyczą w dużej mierze upowszechnienia się wykorzystania cyfrowych danych.

Doskonałym przykładem grupy produktów, które zostały przeobrażone w związku z upowszechnieniem się wykorzystania urządzeń mobilnych i danych cyfrowych, są systemy alarmowe. Przez wiele lat kolejne modele central alarmowych oferowały jedynie obsługę większej niż wcześniej

Rys. 1. Aplikacja do zdalnej obsługi systemu alarmowego

Fot. 1. Mobilna konsola dla ekip patrolujących (fot.: NEXT! s.c.)

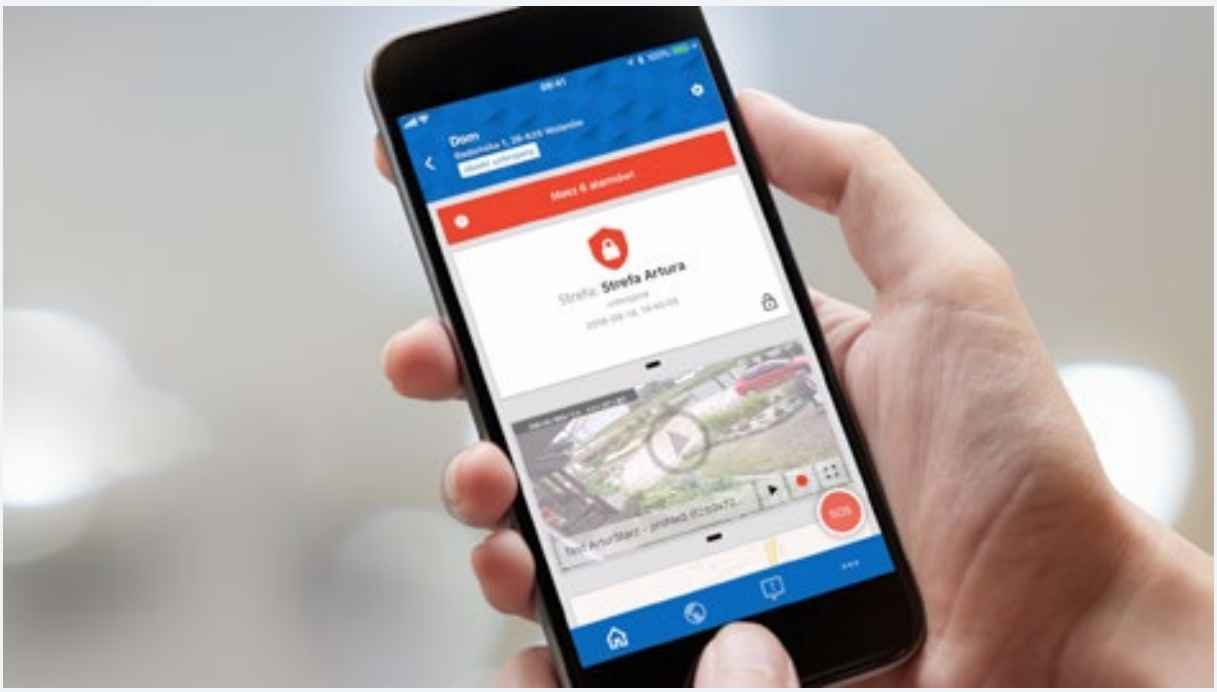
liczby wejść czy wyjść. Ich codzienna obsługa sprowadzała się do korzystania z manipulatorów (początkowo używano prostych klawiatur z wskaźnikami LED, potem pojawiły się również wyświetlacze LCD). Bardziej zaawansowane urządzenia miały intuicyjne w obsłudze graficzne interfejsy użytkownika, jednak w dalszym ciągu sterowanie systemem wymagało podejścia użytkownika do manipulatora. Obecnie systemy alarmowe, które nie współpracują z aplikacjami mobilnymi służącymi do ich zdalnej, wygodnej obsługi, to z reguły konstrukcje przestarzałe. Tak jak piloty do zdalnego sterowania odmieniły na zawsze obsługę telewizorów i innych podobnych urządzeń, aplikacje mobilne do systemów alarmowych powodują zmianę sposobu wykorzystywania tych systemów. Prosta, czytelna i intuicyjna w obsłudze aplikacja sprawia, że system alarmowy przestaje być postrzegany jako coś skomplikowanego. Oczywiście czytelny manipulator z wyświetlaczem jest w dalszym ciągu niezastąpiony w zarządzaniu systemem, ale podstawowa obsługa może być nie tylko prostsza, ale i wygodniejsza, gdy zamiast manipulatora skorzystamy z odpowiedniej aplikacji. Taka obsługa to nie tylko włączanie czy wyłączanie czuwania systemu alarmowego. Nowoczesne centrale alarmowe coraz częściej mają dodatkowe funkcje, np. umożliwiają sterowanie oświetleniem, podnoszeniem i opuszczaniem rolet czy otwieraniem bramy. Takie funkcje mogą być dostępne także dzięki aplikacjom mobilnym oferowanym przez producentów innych nowoczesnych urządzeń. Zmieniają one smartfony w wygodne, uniwersalne urządzenia do zdalnego sterowania.

W nowoczesnym systemie zarządzania stacją monitorowania, w którym odbierane są sygnały z chronionych obiektów, transmitowane są strumienie wizyjne i przekazywane są informacje od pracowników patrolujących teren, możliwości jest jeszcze więcej. Aplikacje mobilne mogą być rozszerzeniem takiego systemu. Dzięki skorzystaniu z aplikacji mobilnej można na przykład mieć wgląd w wysyłane do stacji monitorującej powiadomienia o zdarzeniach alarmowych, informacje o włączeniu albo wyłączeniu czuwania, o awarii itp. Jeśli użytkownik widzi, że sygnały prawidłowo docierają do operatora stacji monitorującej, ochrona staje się dla niego bardziej weryfikowalna, co z jego punktu widzenia może potwierdzać realną wartość usługi i umacnia zaufanie do usługodawcy.

W przypadku zaawansowanych central alarmowych umożliwiających pełną integrację z systemami stacji monitorujących możliwe jest zdalne sterowanie urządzeniami z poziomu aplikacji mobilnej. Dzięki uruchomieniu alarmu za pomocą urządzenia mobilnego można szybko wezwać pomoc wtedy, gdy jest ona najbardziej potrzebna. Na dodatek, dzięki geolokalizacji, dostępna będzie informacja o położeniu urządzenia przenośnego i jego użytkownika, który wzywa pomoc.

Równie istotna dla użytkowników jest funkcja umożliwiająca błyskawiczne odwołanie interwencji w sytuacji, gdy sygnał alarmowy został wywołany z powodu błędu użytkownika. Dzięki temu klient nie zostanie obciążony kosztami interwencji, a agencja ochrony może bardziej optymalnie zarządzać swoimi zasobami.

Aplikacje mobilne to nie tylko narzędzia dla osób korzystających z usług firm ochrony. Odpowied-



Fot. 2. Integracja danych z systemów alarmowych i wizyjnych systemów dozorowych w aplikacji stacji monitorującej (fot.: DMSI SOFTWARE Sp. z o.o.)

nie rozwiązania software'owe wykorzystujące możliwości mobilnych terminali internetowych mogą być świetnymi narzędziami usprawniającymi funkcjonowanie agencji. Dzięki takim aplikacjom ekipy patrolowe mogą mieć na bieżąco aktualizowane, szczegółowe informacje o obiekcie, w którym ma być przeprowadzona interwencja. Narzędzia nawigacyjne wykorzystujące GPS umożliwiają szybsze dotarcie na miejsce interwencji dzięki uwzględnieniu warunków drogowych, a także ułatwiają uzyskanie informacji o położeniu pozostałych załóg interwencyjnych wówczas, gdy potrzebne jest dodatkowe wsparcie. Ważna może być również możliwość komunikacji z operatorami stacji, którzy mogą przekazywać ekipom patrolowym dodatkowe, potrzebne do sprawnej realizacji interwencji informacje. Również późniejsze raportowanie, dzięki rejestrowaniu i dokumentowaniu w urządzeniach przenośnych, może zapewnić bogatszy materiał operacyjny.

Aplikacje mobilne muszą być wspierane nie tyko przez infrastrukturę telekomunikacyjną, ale także przez systemy gwarantujące błyskawiczny dostęp do niezbędnych informacji. Mogą korzystać z chmury obliczeniowej. Urządzenia stają się wówczas multimedialnymi terminalami dla użytkowników, a dane są przetwarzane na zewnątrz przez systemy informatyczne usługodawców, w centrach przetwarzania danych (które muszą być odpowiednio zabezpieczone przed atakami hakerskimi).

Jaki będzie kierunek dalszego rozwoju aplikacji mobilnych w branży zabezpieczeń? Z pewnością urządzenia przenośne w dalszym ciągu będą ułatwiać zdalne sterowanie. Mogą też w jeszcze większym stopniu usprawniać pracę techników i serwisantów. Prawdopodobnie będą odgrywały ważniejszą rolę w zapewnianiu bezpieczeństwa osobistego – w połączeniu z urządzeniami nasobnymi (ang. *wearables*) aplikacje umożliwią na przykład monitorowanie zachowań osób starszych lub wymagających kontroli ze względu na stan zdrowia. Dostęp za pomocą smartfonów do tzw. rozszerzonej rzeczywistości pozwoli na przeniesienie działań ekip interwencyjnych na zupełnie inny, nieosiągalny wcześniej poziom. Interwencja fizyczna w obiekcie połączona z przesyłaniem na żywo obrazu termowizyjnego z drona to już teraźniejszość. Ciekawe, co przyniesie nam przyszłość.

Michał Konarski

Przeprowadzanie audytu

zarządzania bezpieczeństwem organizacyjno-technicznym obiektów. Część 6

Prowadzenie audytu. Praktyka i wytyczne

dr inż. Andrzej Wójcik

Wstęp

Na wstępie należy poinformować, że pojawiły się nowe wersje norm, które mają związek z audytowaniem i które zostały przywołane w poprzednich częściach. Wydano nowa normę PN-EN ISO 19011:2018 *Wytyczne dotyczące auditowania systemów zarządzania*, która zastąpiła normę PN-EN ISO 19011:2012. Wprowadzono też normę PN-ISO 31000:2018 *Zarządzanie ryzykiem. Wytyczne*, która zastąpiła normę PN-ISO 31000: 2012. W celu zwrócenia uwagi na to, że zaszły zmiany w zarządzaniu bezpieczeństwem, należy przypomnieć, że norma PN-EN ISO/ICE:2014 została zastąpiona przez normę PN-EN ISO/ICE:2017 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji.*

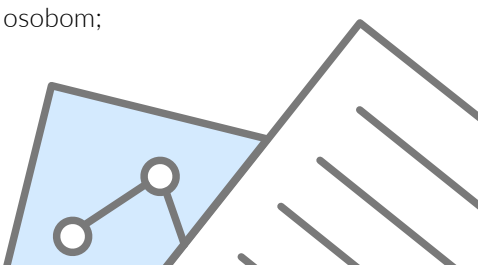
Przeprowadzanie audytu zgodnie z nowymi wymaganiami normatywnymi

Wytyczne normy PN-EN ISO 19011:2018 (w skrócie ISO 19011) są skierowane są do zarządzających programami audytów, do audytorów, a także do jednostek certyfikujących. Normą ISO 19011 mogą kierować się wszystkie organizacje, które planują i przeprowadzają audyty (wewnętrzne lub zewnętrzne) systemów zarządzania lub zarządzają programem audytów. Stosowanie się do wytycznych ISO 19011 w innych rodzajów audytów jest możliwe pod warunkiem, że zwróci się szczególną uwagę na potrzebne specyficzne kompetencje.

Wymagane kompetencje w przypadku audytowania zabezpieczenia organizacyjno-technicznego obiektów, czyli – ogólnie – infrastruktury bezpieczeństwa, obejmują m.in. przygotowanie z zakresu systemów alarmowych – wiedzę o projektowaniu, eksploatacji, serwisie, konserwacji, szacowaniu ryzyka, a także znajomość odpowiednich podstaw normatywnych, prawnych i specyficznych wymagań biznesowych lub korporacyjnych, które mają związek z bezpieczeństwem.

Należy podkreślić, że audyt stanowi skuteczny i niezawodny instrument wspierający politykę bezpieczeństwa obiektu i umożliwiający skontrolowanie zarządzania bezpieczeństwem. Dostarcza informacji, które są niezbędne, by zadbać o bezpieczeństwo w organizacji. W przeprowadzaniu audytu ważne są:

- uczciwość – przede wszystkim prawość, rzetelność, sumienność, niedopuszczenie do przekłamań;
- rzetelność – precyzyjność, dokładność, poprawność przeprowadzenia audytu, a także powtarzalność metodyki;
- profesjonalizm w działaniu – wykonywanie czynności audytowych zgodnie z wymaganiami, fachowość;
- poufność – uzyskane podczas audytu dane nie powinny być ujawnione lub udostępnione nieuprawnionym osobom;



– niezależność – audyt nie może być przeprowadzony w czyimś partykularnym interesie, należy zadbać o bezstronność i oceniać obiektywnie, audytor nie może audytować własnej pracy i być organizacyjnie podległy audytowanemu;
– ustalenie faktów – sprawdzenie aktualnego stanu rzeczy i ustalenie przeszłych zdarzeń, np. sprawdzenie zapisów w dokumentacji czy w rejestrze wydarzeń centrali alarmowej, wywiad z audytowanym;
– uwzględnienie trudności i określenie prawdopodobieństwa, że cele audytu zostaną osiągnięte (ta zasada jest narzucona przez normę ISO 19011).

Należy przestrzegać powyższych zasad, aby wyniki audytu były jednoznaczne i aby można było spodziewać się, że inni audytorzy uzyskają podobne wyniki w podobnych okolicznościach.

Na czym polega uwzględnienie trudności? Audytor powinien dokonać analizy ryzyka i możliwości związanych z realizacją przygotowanego programu audytu w konkretnym przypadku. Audytor powinien określić potencjalne trudności, a z drugiej strony ocenić prawdopodobieństwo przeprowadzenia audytu z powodzeniem, czyli prawdopodobieństwo osiągnięcia celu audytu.

Trudności wynikające z braku oceny ryzyka nieprawidłowego przeprowadzenia audytu mogą być związane przede wszystkim z:
– zaplanowaniem audytu, błędnym określeniem celów audytu (np. sprawdza się stan techniczny wyłącznie wybranych elementów zabezpieczających, a nie to, czy cały obiekt jest odpowiednio zabezpieczony) oraz zakresu programu audytu;
– rozdysponowaniem zasobów i czasem (np. wybrano niekompetentnych przedstawicieli audytowanego lub nie przeznaczono wystarczającego czasu na przygotowanie programu audytu), a także z przeprowadzeniem audytu;
– wyborem zespołu audytującego (np. audytorzy wewnętrzni nie mają kompetencji, aby przeprowadzić audyt skutecznie; nie ma audytora wiodącego, czyli osoby kierującej zespołem przeprowadzającym audyt, lub eksperta technicznego w dziedzinie systemów alarmowych);
– przepływem informacji pomiędzy audytorem a audytowanym (np. brak potwierdzenia programu audytu przez audytowanego);
– zapisami w dokumentacji audytowej, w notatkach audytora (niedokładne opisy, nieodpowiednia ochrona zapisów dotyczących audytu);
– dostępnością dowodów (dokumentacji dotyczącej zabezpieczeń w obiekcie, dziennika konserwacji systemów alarmowych, rejestrów central alarmowych itd.);
– uwzględnieniem zmian organizacyjnych (np. zmian lokalizacji, zmian w kierownictwie orga-

nizacji, zmian w przepisach prawnych, którym podlega organizacja i które mają wpływ na program oraz wynik audytu);

Wyróżniamy audyty wewnętrzne, zwane inaczej audytami pierwszej strony, oraz audyty zewnętrzne, które możemy podzielić na audyty drugiej strony, np. dostawcy usług, i audyty trzeciej strony, np. organizacji certyfikujących.

Rodzaje audytów mających związek z bezpieczeństwem:
- audyt usługi – może dotyczyć na przykład projektowania, instalacji, konserwacji i serwisu systemu alarmowego, a także dostawy produktów (w tym przypadku zabezpieczeń);
- audyt procesu – może dotyczyć na przykład realizacji i skuteczności procesu projektowania, instalacji, konserwacji i serwisowania systemu alarmowego, a także dostawy produktów (w tym przypadku zabezpieczeń),
- audyt systemu – możemy audytować system zabezpieczeń organizacyjno-technicznych ogólnie, ale także wybrane systemy zabezpieczeń, np. kontroli dostępu czy CCTV.

Należy pamiętać, że audyt zarządzania bezpieczeństwem obiektów, szczególnie prowadzony przez strony zewnętrzne, może dotyczyć dostawy, spełnienia wymogów dotyczących gwarancji na urządzenia czy usługę oraz serwisowania urządzeń alarmowych.

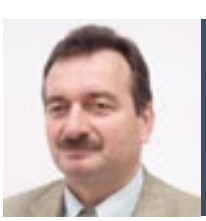
Ważnym zagadnieniem jest podejście procesowe podczas realizacji audytu. Zastosowanie podejścia procesowego, czyli przeprowadzenie kompletnej kontroli funkcjonowania systemu zarządzania bezpieczeństwem w obiekcie (kontroli m.in. organizacji ochrony, zabezpieczeń technicznych, sposobu eksploatacji), wynika z dyrektywy ISO/IEC (część 1, załącznik SI). Audytorzy powinni prowadzić audyt systemu zarządzania procesami w organizacji i wzajemnej relacji tych procesów w odniesieniu do jednego lub więcej standardów zarządzania, np. zarządzania bezpieczeństwem obiektów zgodnie z ISO27001 i ciągłością procesów związanych z zaopatrzeniem w energię zgodnie z ISO 22301.

W następnej części opiszę przygotowywanie planu audytu, przykładowe aspekty audytowania bezpieczeństwa obiektów i to, w jaki sposób korzystać z różnych źródeł informacji.

Dobrowolne stosowanie Polskich Norm w praktyce

Należy podkreślić, że zacytowane we wstępie normy są wydane w języku oryginału. Tylko tytuły na okładkach są przetłumaczone na język polski. W związku z tym możliwe są różne interpretacje poszczególnych zapisów, co stanowi problem. Wielokrotnie podczas różnych audytów i szkoleń odbiorcy pytali mnie, dlaczego tak ważne normy są wydawane tylko i wyłącznie w języku oryginału. Problem ten reguluje ustawa z dnia 12 września 2002 r. o normalizacji (Dz. U. Nr 169, poz. 1386 ze zm.) – w art. 5. 1 znajduje się następujący zapis: „Polska Norma jest normą krajową, przyjętą w drodze konsensu i zatwierdzoną przez krajową jednostkę normalizacyjną, powszechnie dostępną, oznaczoną – na zasadzie wyłączności – symbolem PN".

Norma europejska lub międzynarodowa może być wprowadzona w Polsce w języku oryginału jako norma obowiązująca (może stać się Polską Normą). Stosowanie Polskich Norm jest dobrowolne. Polskie Normy mogą być przywoływane w przepisach prawnych po ich opublikowaniu w języku polskim. Do czasu opublikowania nowej normy napisanej w języku polskim obowiązuje norma dotychczasowa. Norma w języku oryginału może być stosowana tylko na zasadzie uznaniowej.



Andrzej Wójcik

Opracował
dr inż. Andrzej Wójcik
ekspert i rzeczoznawca ds. bezpieczeństwa technicznego i ochrony informacji
audytor ds. bezpieczeństwa biznesu
andrzejw@esinstal.pl

Współpraca firm AxxonSoft i Intel

AxxonSoft

Tworzenie inteligentnych systemów zabezpieczających i dozorowych dostosowanych do rozległych obszarów publicznych stanowi poważne wyzwanie. Przykładem mogą być stadiony i inne miejsca w przestrzeni miejskiej, w których organizowane są imprezy sportowe o randze światowej, koncerty popularnych gwiazd muzyki rockowej czy inne imprezy ściągające wielotysięczne tłumy uczestników. Organizatorom takich imprez trzeba dać narzędzia umożliwiające skuteczną realizację procedur bezpieczeństwa. W tym celu angażowane są środki techniczne w postaci rozbudowanych systemów zabezpieczeń elektronicznych. Główną rolę odgrywają w tym przypadku wizyjne systemy dozorowe.

Jeśli weźmie się pod uwagę czynnik skali, czyli znacznej rozległości i stopnia złożoności takich systemów, łatwo dojść do wniosku, że stopień ich automatyzacji musi być bardzo wysoki. Trudno sobie wyobrazić, że operatorzy systemu składającego się z tysięcy kamer mogą skutecznie wykorzystać jego zalety i wyłonić z tłumu osoby mogące stanowić zagrożenie dla innych, podobnie jak trudno wyobrazić sobie ręczne zarządzanie ruchem bardzo wielu pojazdów. W tak rozległych systemach konieczne jest zastosowanie szybkich sieci umożliwiających transmisję obrazów z kamer do centrów dowodzenia i równie szybkich serwerów, dzięki którym możliwe jest przetwarzanie tak dużych ilości danych. Poważnym problemem jest właściwa ocena sytuacji i unikanie fałszywych alarmów, o które łatwo, gdy rozwój wydarzeń jest dynamiczny.

Koncentracja urządzeń o dużych mocach obliczeniowych w centrach przetwarzania danych jest bardzo kosztowna. Równie kosztowne są sieci umożliwiające szybkie przesyłanie dużych ilości danych, niezawodne sieci zasilające o dużej mocy, infrastruktura do chłodzenia sprzętu i wiele innych składników. Z tych względów znaczenia nabiera przetwarzanie danych w urządzeniach peryferyjnych, jakimi są nowoczesne kamery telewizyjne z rozbudowanymi funkcjami analizy treści obrazu. Nowoczesne rozwiązania sprzętowe i programowe są trudne do zintegrowania ze starymi instalacjami. Często zdarza się, że przestarzały sprzęt jest niejednorodny w swojej strukturze, poszczególne fragmenty pochodzą od różnych producentów i zostały zainstalowane w różnych latach. W takiej sytuacji nie można obejść się bez dodatkowego zainwestowania w sprzęt oraz w odpowiednio wyszkolony personel.

W takich warunkach rozpoczynali pracę organizatorzy dwudziestych pierwszych Mistrzostw Świata w Piłce Nożnej, które odbyły się w Moskwie w 2018 roku. Skala organizacji tej imprezy była ogromna. Udział wzięło wiele agencji, wielu dostawców sprzętu, instalatorów i organizatorów. Tylko w samej Moskwie kompleks olimpijski miał powierzchnię 145 hektarów. W trakcie imprezy trzydzieści dwie drużyny piłkarskie rozegrały sześćdziesiąt cztery mecze na dwunastu stadionach zlokalizowanych w jedenastu rosyjskich miastach. Stadiony odwiedziło ponad trzy miliony kibiców, a ponadto dziesiątki milionów fanów śledziły przebieg rozgrywek w strefach kibica i innych miejscach publicznych.

Zapewnienie bezpiecznego przebiegu tak dużej imprezy wymagało zaangażowania partnerów technologicznych zdolnych sprostać stawianym wymaganiom. Tymi partnerami byli AxxonSoft i Intel – światowi potentaci w dziedzinie nowoczesnej elektroniki.

Konieczne było zastosowanie na wielką skalę najnowszych osiągnięć techniki, w tym systemów wykorzystujących sztuczną inteligencję i zdolność do tzw. głębokiego uczenia się (ang. *deep learning*). Zastosowanie obróbki danych w urządzeniach peryferyjnych pozwoliło na znaczne obniżenie kosztów całej inwestycji.

Oprogramowanie umożliwiające obsługę zintegrowanego systemu zabezpieczeń dostarczyła firma AxxonSoft, zaś producentem i dostawcą kontrolerów peryferyjnych oraz sprzętu serwerowego była firma Intel. Ponadto w celu realizacji funkcji głębokiego uczenia się w urządzeniach peryferyjnych zastosowane zostały narzędzia programowe OpenVINO.

Jednym z ważnych elementów oprogramowania AxxonSoft wykorzystywanego podczas mistrzostw piłkarskich w Moskwie był system rozpoznawania i identyfikacji twarzy. Tego typu systemy są stosowane do ochrony antyterrorystycznej podczas imprez masowych. Dzięki nim możliwe jest wykrywanie prób wtargnięcia na tereny stadionów przez osoby mające sądowy zakaz wstępu na imprezy masowe.

Na terenach przyległych do obiektów sportowych zainstalowano systemy do kontroli ruchu pojazdów, w tym systemy do rozpoznawania i odczytu danych z tablic rejestracyjnych pojazdów. Pozwoliło to usprawnić obsługę dróg dojazdowych i parkingów.

W systemie użyto ponad dziewięciu tysięcy kamer rozmieszczonych we wszystkich miastach, w których odbyły się rozgrywki. System został zintegrowany z instalacją wizyjną utworzoną na użytek rosyjskiego ministerstwa spraw wewnętrznych. Punkty dowodzenia zostały rozmieszczone w pobliżu poszczególnych obiektów sportowych.

Wykorzystano fragmenty istniejących, utworzonych w różnych okresach instalacji zabezpieczających różnych producentów. Oprogramowanie AxxonSoft umożliwiło integrację tych instalacji i utworzenie jednego, spójnego systemu zabezpieczeń.

Do obsługi tak rozległego wizyjnego systemu dozorowego posłużył ujednolicony interfejs graficzny bazujący na oprogramowaniu AxxonSoft działającym na sprzęcie firmy Intel. Zastosowanie ujednoliconego interfejsu we wszystkich punktach dowodzenia ułatwiło obsługę systemu i pozwoliło na uniknięcie pomyłek wynikających z niejednorodności starych i nowych rozwiązań.

Główne zalety systemów firmy AxxonSoft działających na sprzęcie firmy Intel:

- otwarta platforma (integruje wszystkie systemy bezpieczeństwa, oprogramowanie i urządzenia –zarówno nowe, jak i starszego typu – i uruchamia je we wspólnym środowisku);
- skalowalność (umożliwia połączenie różnych systemów – niezależnie od typu, producenta, parametrów technicznych);
- inteligencja (umożliwia wiarygodną interpretację danych i zdarzeń; zapewnia szybkie, automatyczne reakcje na wykryte zagrożenia nawet w gęsto zaludnionym środowisku);
- modułowość (systemy składają się z modułów funkcjonalnych, takich jak POS, LPR, rozpoznawanie twarzy, co upraszcza rozwiązywanie konkretnych problemów);
- niezawodność (platformą, na której działa oprogramowanie AxxonSoft, są produkty firmy Intel; jest to podstawą niezawodności działania złożonych systemów zawierających bardzo wiele kamer).

Przewodniczący organizacji FIFA Gianni Infantino nazwał zeszłoroczne Mistrzostwa Świata w Piłce Nożnej najlepszymi w historii. Oprócz tego wysoko ocenił jakość infrastruktury i poziom bezpieczeństwa na stadionach.

AxxonSoft
Tłumaczenie: Andrzej Walczyk

RACS 5

Skalowalny system bezpieczeństwa, automatyki i kontroli dostępu

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

- Identyfikacja mobilna (Bluetooth, NFC, QR)
- Identyfikacja biometryczna za pośrednictwem linii papilarnych
- Identyfikacja za pośrednictwem tablic rejestracyjnych
- Integracja z systemem alarmowym
- Integracja CCTV (HIKVISION, DAHUA, ONVIF)
- Integracja z zamkami bezprzewodowymi APERIO (ASSA ABLOY)
- Integracja z zamkami bezprzewodowymi RWL (ROGER)
- Kontrola dostępu do parkingów
- Kontrola dostępu do pokoi hotelowych
- Kontrola dostępu do wind klasycznych
- Kontrola dostępu do wind KONE
- Kontrola dostępu do szafek
- Monitorowanie obiegu przedmiotów w tym kluczy
- Kontrola uprawnień do wypożyczenia przedmiotów
- Obsługa sprzedaży towarów i usług (PoS)
- Obsługa drukarek kart
- Zarządzanie i konfigurowanie z poziomu aplikacji Windows (VISO ST i EX)
- Zarządzanie z poziomu aplikacji webowej (VISO Web)
- Zarządzanie z poziomu aplikacji mobilnej (VISO Mobile)
- Serwer Integracji

Wysoka niezawodność i funkcjonalność potwierdzona w tysiącach wdrożonych z sukcesem instalacji w Polsce i za granicą.

roger®
Intelligence for Building

NVR-6332-H8/FR

Rejestrator z funkcją RAID

Nowy model rejestratora **NVR-6332-H8/FR** ma funkcję **RAID** rekomendowaną dla obiektów o wysokich wymaganiach dotyczących bezpieczeństwa. Zastosowanie funkcji RAID, w zależności od konfiguracji, pozwoli zwiększyć niezawodność systemu (odporność na awarię dysków) oraz wydajność zespołu dysków, a także powiększyć przestrzeń dyskową dostępną jako jedna całość.

Wizja	
Kamery IP	do 32 kanałów w rozdzielczości 3840 x 2160 (obraz + dźwięk)
Obsługiwana rozdzielczość	maks. 3840 x 2160
Kompresja	H.264, H.264+, H.265
Wyjścia monitorowe	główne (podział, pełny ekran, sekwencja): 1 x VGA, 1 x HDMI (4K Ultra HD) spot: 1 x HDMI (Full HD)
Dwustrumieniowość	tak
Obsługa kamer fisheye	tak, kamery IP serii 3000
Nagrywanie	
Prędkość nagrywania	960 kl./s (32 x 30 kl./s dla 3840 x 2160 i niższych)
Wielkość strumienia	256 Mb/s łącznie ze wszystkich kamer
Odtwarzanie	
Prędkość odtwarzania	480 kl./s (16 x 30 kl./s dla 3840 x 2160) *
Dyski	
Wewnętrzne	możliwość montażu: 8 x HDD 3.5" 10 TB SATA *
Maksymalna wewnętrzna pojemność	80 TB
Tryb RAID	RAID0, RAID1, RAID5, RAID6
Alarmy	
Wejścia/wyjścia alarmowe lokalne	8/4 typu przekaźnikowego
Wejścia/wyjścia alarmowe w kamerach	obsługa wejść/wyjść dostępnych w kamerach*
Detekcja ruchu	obsługa funkcji detekcji ruchu dostępnej w kamerach*
Reakcja na zdarzenia alarmowe	sygnał dźwiękowy, e-mail, aktywacja wyjścia alarmowego, aktywacja nagrywania, PTZ
Inteligentna analiza obrazu	
Obsługiwane funkcje	sabotaż, zmiana sceny, utrata ostrości, zmiana kolorystyki, przekroczenie linii, wkroczenie do strefy, pojawienie się obiektu, zniknięcie obiektu, rozpoznawanie twarzy
Sieć	
Interfejs sieciowy	2 x Ethernet - złącze RJ-45, 10/100/1000 Mbit/s
Wsparcie protokołu ONVIF	Profile S (ONVIF 2.2 lub wyższy)
Programy na PC/MAC	NMS, Internet Explorer, NVR-6000 Viewer/Safari
Programy na smartfonie	SuperLive Plus (iPhone, Android)
Maks. liczba połączeń z rejestratorem	4
Dodatkowe interfejsy	
Porty USB	2 x USB 2.0, 1 x USB 3.0
Parametry instalacyjne	
Mocowanie RACK 19"	2U

* Przy wykorzystaniu dwustrumieniowości.

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

NVS-3116SP

Przełącznik 16-portowy z funkcją PoE

Wszystkie modele przełączników marki NOVUS spełniają wymagania standardu IEEE802.3af, pozwalają na zasilanie urządzeń podłączonych do wszystkich portów przełącznika metodą PoE. Obciążalność dla wszystkich portów znacznie przekracza wartość określoną przez standard (15,4 W) i dochodzi do 30 W dla dowolnego portu.

Informacje ogólne	
Typ urządzenia	Przełącznik sieciowy z funkcją PoE
Sieć	
Porty zewnętrzne	Porty PoE: 16 x 10 Mb/s / 100 Mb/s Port UPLINK 1 Gb/s: 1 Uplink Combo x 1 :SFP(1Gb/s) + RJ45(1Gb/s)
Zgodność ze standardami PoE	IEEE802.3 af, IEEE802.3 at
Tryb zasilania PoE	Endspan (1,2+ / 3,6-)
Łączna przepustowość	7.2 Gb/s
Obsługiwane protokoły	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z
Lista adresów MAC	4K
Parametry instalacyjne	
Obudowa	Metalowa, kolor granatowy
Wymiary (mm)	280 (szer.) x 44 (wys.) x 180 (dł.)
Masa	1,9 kg
Zasilanie	100 ~ 240 V_{AC}, 50/60 Hz
Pobór mocy	190 W
Wydajność portów	190 W dla portów 1 do 16, nie więcej niż 30 W dla jednego portu
Temperatura pracy	0°C ~ 40°C
Reakcja na zdarzenia alarmowe	e-mail z załącznikiem, zapis na FTP, zapis na kartę SD, aktywacja wyjścia alarmowego
Oświetlacz IR	
Liczba diod/zasięg/kąt świecenia	3/10 m/120°
Interfejsy	
Wejścia/wyjścia akustyczne	+ wbudowany mikrofon
Wejścia/wyjścia alarmowe	1 (NO/NC)/1
Gniazdo kart pamięci	microSD - pojemność do 128 GB
Parametry instalacyjne	
Obudowa	IP66, wandaloodporna aluminiowa, biała
Temperatura pracy	-30°C ~ 55°C

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa

tel. 22 546 05 46, faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

RKD32

Depozytor kluczy w systemie RACS 5

Charakterystyka

- Depozytor elektroniczny na 32 klucze
- Możliwość połączenia do 4 depozytorów w jeden system
- Trwałe zespolenie klucza z brelokiem przez użytkownika systemu
- Możliwość stosowania dodatkowych plomb łączących klucz z brelokiem
- Mechaniczna blokada pobrania klucza
- Identyfikator radiowy klucza wewnątrz breloka
- Harmonogramy czasowe uprawniające do pobrania kluczy
- Rejestracja obiegu kluczy
- Swobodny dostęp do kluczy w tzw. trybie biurowym
- Funkcja rezerwacji kluczy
- Odczyt aktualnego statusu klucza
- Zarządzanie z poziomu panelu dotykowego 7”
- Obudowa metalowa z przeszklonymi drzwiami
- Awaryjne odblokowanie kluczy po komisyjnym otwarciu obudowy depozytora
- Praca autonomiczna lub w ramach systemu RACS 5
- Zasilanie zewnętrzne 12 V

roger®
Intelligence for Building

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

RCP Point

Program do rejestracji czasu pracy

RCP Point to aplikacja na smartfon i tablet, która wykorzystuje funkcję NFC i sprawia, że urządzenie mobilne może działać jako terminal rejestracji czasu pracy. Aplikacja działa na urządzeniu mobilnym z systemem operacyjnym Android lub przeznaczonym do tego celu stacjonarnym panelu dotykowym MD70 (ROGER). Zdarzenia zarejestrowane w aplikacji RCP Point są przekazywane do programu RCP Master 3 (Windows), który umożliwia konfigurowanie ustawień rejestratora oraz tworzenie szczegółowych raportów z uwzględnieniem zasad obowiązujących w danym miejscu pracy. Program RCP Master może obsługiwać wiele rejestratorów, w tym rejestratory pracujące autonomicznie, użytkowane poza siecią komputerową w której funkcjonuje program RCP Master 3 i tylko okresowo dołączane do tej sieci. W przypadku, gdy rejestrator jest na stałe podłączony do lokalnej sieci komputerowej zdarzenia z rejestratora są na bieżąco i bez udziału operatora przekazywane do bazy danych programu RCP Master 3. Dodatkowo możliwe jest w takim przypadku monitorowanie obecności osób w obiekcie, jak i rodzaju trybu obecności użytkowników rejestrowanego w danej chwili. W przypadku gdy rejestrator jest użytkowany poza lokalną siecią komputerową zdarzenia są buforowane w jego wewnętrznej pamięci i przenoszone do bazy danych RCP Master 3 z chwilą podłączenia do sieci komputerowej. Graficzny panel dotykowy MD70 z fabrycznie zainstalowaną aplikacją RCP Point został zaprojektowany do pracy jako terminal rejestracji czasu pracy. Urządzenie można zamontować na ścianie lub przeznaczonym uchwycie umożliwiającym ergonomiczną obsługę urządzenia. Panel MD70 ma ekran dotykowy o przekątnej 7", kamerę, czytnik zbliżeniowy kart MIFARE oraz interfejsy sieciowe: przewodowy (Ethernet) i bezprzewodowy (Wi-Fi). Aby zarejestrować na terminalu wejście lub wyjście z pracy użytkownik może użyć karty zbliżeniowej lub kodu PIN. Aplikacja pozwala na wybór trybu rejestracji RCP z listy obejmującej 250 pozycji, w skład której wchodzą predefiniowane tryby RCP (wejście, wyjście, wyjście służbowe) jak i własne tryby RCP zdefiniowane stosownie do potrzeb danej instalacji (wyjście na urlop, wyjście do palarni, wyjście do bufetu itp.). Aplikacja RCP Point może wykonywać zdjęcia osób rejestrujących wejście lub wyjście, co w znaczny sposób zabezpiecza system przed próbami rejestracji przy użyciu identyfikatorów należących do innych osób i omijania w ten sposób zasad regulaminu pracy. Terminal rejestracji czasu dzięki urządzeniu mobilnemu z programem RCP Point i programem RCP Master 3 tworzą autonomiczny zestaw umożliwiający elektroniczną rejestrację i raportowanie czasu pracy.

Charakterystyka

- Rejestracja czasu pracy i obecności
- 250 trybów rejestracji
- Identyfikacja użytkowników za pomocą kodów PIN
- Identyfikacja użytkowników za pomocą kart zbliżeniowych MIFARE (MD70)
- Pamięć 300 000 zdarzeń (30 000 zdarzeń ze zdjęciem)
- Obsługa 1 000 użytkowników
- Zdjęcia osób rejestrujących wejście lub wyjście
- Kontrola obecności twarzy za pomocą kamery
- Komunikacja poprzez sieć komputerową (Ethernet, Wi-Fi)
- Szyfrowana transmisja danych
- Współpraca z programem RCP Master 3

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum, woj. Pomorskie

tel. 55 272 0132, faks 55 272 0133
e-mail: roger@roger.pl
http://www.roger.pl

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

Oddziały:
ul. Koniczynowa 2A, 03-612 Warszawa II
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Antoniuk Fabryczny 22, 15-741 Białystok
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@aat.pl

ul. Łęczycka 37, 85-737 Bydgoszcz
tel./faks 52 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 Katowice
tel./faks 32 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 Kielce
tel./faks 41 361 16 32, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 Kraków
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Energetyków 13a, 20-468 Lublin
tel. 81 744 93 65/66; faks 81 744 91 77
e-mail: aat.lublin@aat.pl

ul. Dowborczyków 25, 90-019 Łódź
tel./faks 42 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 Poznań
tel./faks 61 662 06 60, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 81-855 Sopot
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

ul. Zielona 42, 71-013 Szczecin
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

ul. Na Niskich Łąkach 26, 50-422 Wrocław
tel./faks 71 348 20 61, 348 42 36
e-mail: aat.wroclaw@aat.pl

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44; faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85; faks 22 833 87 95
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

ALARMTECH POLSKA Sp. z o.o.
Oddział w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40; faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

ALARM-TECH Systemy Zabezpieczeń s.c.
ul. Graniczna 4
32-086 Boleń
tel. kom. 775 453 453
e-mail: sklep@napad.pl
www.napad.pl

Oddział:
os. Jagiellońskie 19, 31-834 Kraków
tel. kom. 609 197 800

ASSA ABLOY POLAND Sp. z o.o.
ul. Jana Olbrachta 94
01-102 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 41 00, faks 22 715 41 05
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
Tel. kom. 604 569 775
e-mail: brabork@braborklab.pl
www.braborklab.pl

bt electronics Sp. z o.o.
ul. Dukatów 10
31-431 Kraków
tel./faks 12 410 85 10
e-mail: bte@bte.pl
www.bte.pl

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17; faks 22 855 00 19
e-mail: biuro@cs.pl
www.cs.pl

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. K.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00; faks 12 423 44 61
e-mail: office@dyskret.com
www.dyskret.com

EBS Sp. z o.o.
ul. B. Czecha 59
04-555 Warszawa
tel. 22 518 84 00; faks 22 518 84 99
e-mail: sales@ebs.pl
https://www.ebssmart.com

ELTROX
ul. Główna 23
42-280 Częstochowa
tel. 34 333 57 04
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Św. Rocha 87, 42-202 Częstochowa
tel. 34 333 57 13
e-mail: czestochowa@eltrox.pl

ul. Hynka 6/2, 80-465 Gdańsk
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. Myśliborska 2-6, 66-400 Gorzów Wlkp.
tel. 95 766 65 16
e-mail: gorzow@eltrox.pl

ul. Wybickiego 42a, 31-302 Kraków
tel. 12 210 06 25
e-mail: krakow@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 233 49 96
e-mail: lodz@eltrox.pl

ul. Orla 7/I, 41-205 Sosnowiec
tel. kom. 501 945 219
e-mail: sosnowiec@eltrox.pl

ul. ks. kard. S. Wyszyńskiego 22
70-203 Szczecin
tel. 91 443 56 36
e-mail: szczecin@eltrox.pl

ul. Joachima Lelewela 33, 87-100 Toruń
tel. 56 645 94 24
e-mail: torun@eltrox.pl

ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

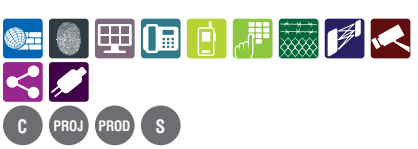
ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 504 904 689
e-mail: wroclaw@eltrox.pl

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

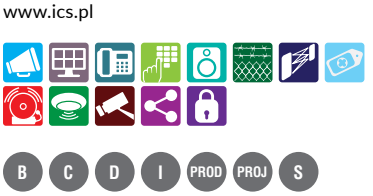
FES TRADING Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44; faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl

GDE POLSKA
Leszek Mitusiński
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35;
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

HANWHA TECHWIN EUROPE LTD.
Biuro w Polsce
ul. Posag 7 Panien 1
02-495 Warszawa
Tel. kom. 518 346 039
e-mail: k.dulin@hanwha.com
https://www.hanwha-security.eu/pl/



ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38; faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl



INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79, 411 57 47; faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53; faks 22 863 74 23
e-mail: janex@janexint.com.pl
www.janexint.com.pl

KATON Sp. z o.o.
ul. Bajana 31E
01-904 Warszawa
tel. 22 869 43 92; faks 22 869 43 93
e-mail: biuro@katon.eu
www.katon.eu

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
www.micromade.pl

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
e-mail: info@micronix.pl
www.micronix.pl

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61; faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@profisystems.pl
www.profisystems.pl

RAMAR s.c.
ul. Modlińska 237
03-120 Warszawa
Tel. 22 676 77 37, 676 82 87
e-mail: ramar@ramar.com.pl
www.ramar.com.pl

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22; faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16; faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

SCHRACK SECONET POLSKA Sp. z o. o.
Wilanów Office Park, bud. B1
ul. Adama Branickiego 15
02-972 Warszawa
tel./faks 22 33 00 620/624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. M. Gomółki 2, 80-279 Gdańsk
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17
(wejście od ul. Stawowej)
31-358 Kraków
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

ul. Św. Czesława 7 lok. 18, 61-575 Poznań
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

TAP - Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
faks 22 625 26 75
e-mail: techom@techom.com
www.techom.com

W2 Włodzimierz Wyrzykowski
ul. Czajcza 6
86-005 Białe Błota
tel. 52 345 45 00
e-mail: biuro@w2.com.pl
www.w2.com.pl

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

VIASAT MONITORING Sp. z o.o.
ul. Puławska 359
02-801 Warszawa
tel. 22 546 0 888; faks 22 546 0 619
e-mail: info@viasat.com.pl
www.viasat.com.pl

Oddziały:
ul. Składowa 2, 41-902 Bytom
tel. 32 388 09 50; faks 32 388 09 60

ul. Zatorska 36, 51-215 Wrocław
tel. kom. 697 972 558
faks 71 341 16 26

ul. Nowy rynek 2, 62-002 Suchy Las k/Poznania
tel. kom. 601 410 979, 601 203 664

ul. Hallera 140, lok. 124, 80-416 Gdańsk
tel kom. 693 694 339

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie www.zabezpieczenia.com.pl

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Arkadiusz Milka
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

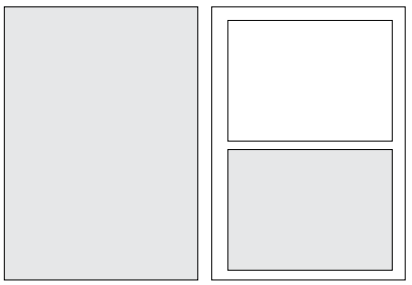
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

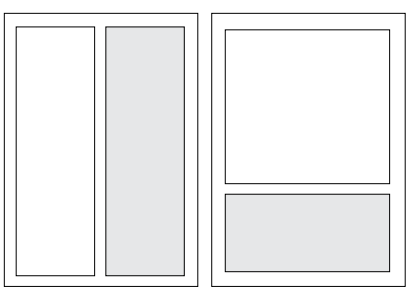
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



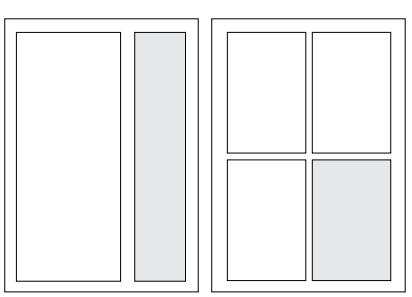
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

EVIX®

MADE IN EU

NOWY WYMIAR OCHRONY
CZUJKI DUALNE PIR + MW

IDEALNE UZUPEŁNIENIE KAŻDEGO SYSTEMU ALARMOWEGO

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

BOSCH
Technologia bliżej nas

FLEXIDOME IP starlight 8000i.
Najwyższy poziom szczegółowości dla zachowania wysokich standardów bezpieczeństwa.

Kamery FLEXIDOME IP starlight 8000i dzięki innowacyjnej koncepcji montażu i zdalnej konfiguracji skracają czas instalacji i uruchomienia nawet o 75%. Rozdzielczość obrazu do 4K UltraHD, w połączeniu z technologią Starlight, zapewniają najwyższą jakość obrazu, a wbudowane funkcje analizy obrazu IVA gwarantują najwyższą skuteczność alarmowania, znacznie podnosząc poziom bezpieczeństwa.

Dowiedz sie więcej na **www.boschsecurity.pl**