OCHRONA i BEZPIECZEŃSTWO OBIEKTÓW I BIZNESU

Nr 3/2022 maj/czerwiec
Cena 15,00 (w tym 8% VAT), ISSN 2658-1779, nr ind. 381756

ISSN 2658-1779
9 772658 177205 06

NOWOŚĆ

Zewnętrzny sygnalizator głosowo - optyczny

SGO-Pgz3

GŁOŚNIEJSZY, JAŚNIEJSZY, LEPSZY

20 Wykorzystanie posiadanego sprzętu przez funkcjonariuszy Służby Więziennej jako istotny element podnoszący bezpieczeństwo jednostek organizacyjnych Służby Więziennej
– mjr dr Paweł Łuszcz

28 Zasilacze do urządzeń przeciwpożarowych – wymagania CNBOP
– Robert Gabrysiak

36 Bezpieczeństwo pożarowe systemów fotowoltaicznych
– Norbert Tuśnio

20 SPIN
EDYCJA JUBILEUSZOWA

Bania ★★★★
HOTEL

20 lat tradycji

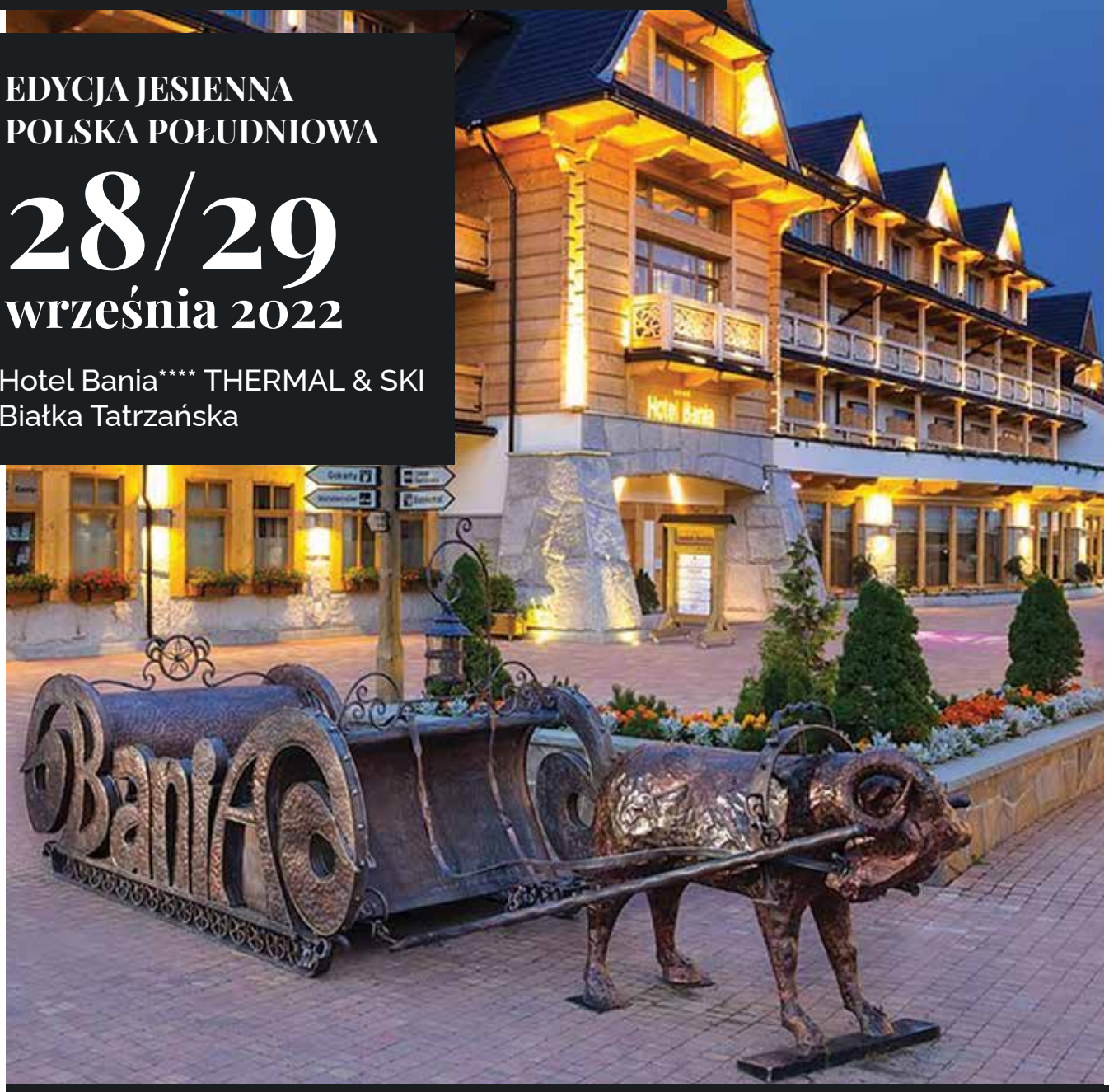
Spotkań Projektantów Instalacji Niskoprądowych

Świętuj z nami jubileusz 20 - lecia SPIN flagowego wydarzenia branży niskich prądów

EDYCJA JESIENNA
POLSKA POŁUDNIOWA

28/29 września 2022

Hotel Bania**** THERMAL & SKI
Białka Tatrzańska



spin.lockus.pl

LOCKUS tel: +48 605 868 610 spin@lockus.pl

Drodzy Czytelnicy!

Rozpoczynamy sezon urlopowy, którego nieodzownym towarzyszem na pewno będzie prezentowany trzeci w tym roku numer Ochrony i Bezpieczeństwa. Wydanie to może stanowić doskonałą lekturę na czas urlopu i wypoczynku.

A co w numerze? Przede wszystkim zapraszam do zapoznania się z relacjami z targów SECUREX oraz POLSECURE. Poza tym w dziale aktualności znajdziemy wiele nowych ciekawostek z branży ochrony i bezpieczeństwa. Dodatkowo jak to bywa w każdym naszym numerze, oferujemy Wam ciekawe artykuły z branż: CCTV, więziennictwa, cyberbezpieczeństwa a także PPOŻ w odniesieniu do systemów fotowoltaicznych.

Jak zwykle gwarantujemy wysoką jakość zamieszczonych artykułów wynikającą z wiedzy i fachowości ich autorów. Wierzymy, że prezentowany numer OiB spełni Państwa oczekiwania i każdy znajdzie w nim coś interesującego.

Życząc pięknej pogody podczas urlopu oraz aktywnego wypoczynku – zachęcam w chwilach spokoju i relaksu do lektury naszego czasopisma.

Robert Gabrysiak
Redaktor prowadzący

Reklama

Patronat Honorowy
Prezydenta Rzeczypospolitej Polskiej
Andrzeja Dudy

Partner strategiczny
PGZ

Targi Kielce
exhibition & congress centre

30 LAT mspo

ufi Member

RELACJE KONTAKTY BIZNES

Międzynarodowy Salon Przemysłu Obronnego
6-9 / 09 / 2022

WYSTAWA
NARODOWA TURCJI

www.mspo.pl

AKTUALNOŚCI I INFORMACJE BRANŻOWE

3 **20 SPIN Jubileuszowe Spotkanie Projektantów Instalacji Niskoprądowych 28–29 września w Hotelu BANIA**

4 **10-lecie CIAS Polska – Jubileuszowa relacja z Pałacu w Małej Wsi**

5 **Jak kompleksowo dbać o bezpieczeństwo w branży przemysłowej? – AXIS Communications**

6 **POLSECURE 2022 – relacja z Międzynarodowych Targów Policji i Bezpieczeństwa Publicznego w Kielcach**

8 **SECUREX 2022 – relacja z Międzynarodowych Targów Zabezpieczeń SECUREX w Poznaniu**

10 **II Ogólnopolskie Warsztaty Reagowania na Zamachy – Dobre Praktyki i Rekomendacje – Aritech i Safety Project**

10 **Nowe głośniki w ofercie AMBIENT SYSTEM**

11 **Nowa Edycja Programu RCP MASTER do Analizy i Rozliczania Czasu Pracy – firmy ROGER**

11 **Przemysłowe Stacje Interkomowe SIP – Trwałe Rozwiązanie Systemowe od C&C Partners**

BEZPIECZEŃSTWO

OCHRONA PRZECIWPOŻAROWA

12 **Ewolucja czy rewolucja? Nowy zewnętrzny sygnalizator głosowo – optyczny typu SGO PGZ3**
[W2]

MONITORING WIZYJNY

14 **Rejestracja obrazu w telewizji dozorowej CCTV**
[Damian Żabicki]

BEZPIECZEŃSTWO JEDNOSTEK PENITENCJARNYCH

20 **Wykorzystanie posiadanego sprzętu przez funkcjonariuszy Służby Więziennej jako istotny element podnoszący bezpieczeństwo jednostek organizacyjnych Służby Więziennej**
[Paweł Łuszcz]

ZABEZPIECZENIA PRZECIWPOŻAROWE

28 **Zasilacze do urządzeń przeciwpożarowych – wymagania CNBOP**
[Robert Gabrysiak]

ANALIZA ZAGROŻEŃ CYBERNETYCZNYCH

32 **Cyber threat intelligence**
[Grzegorz Data]

BEZPIECZEŃSTWO POŻAROWE SYSTEMÓW FOTOWOLTAICZNYCH

36 **Bezpieczeństwo pożarowe systemów fotowoltaicznych**
[Norbert Tuśnio]

MONITORING MIEJSKI

42 **Monitoring wizyjny w przestrzeni publicznej**
[Robert Gabrysiak]

ZARZĄDZANIE

NOWOCZESNE SYSTEMY MONITORINGU WIZYJNEGO

18 **Nowoczesne systemy parkingowe i otwierania szlabanów**
[Robert Gabrysiak]

KONTROLA DOSTĘPU

26 **Nowoczesny system kontroli dostępu bez kłopotu**
[WINKHAUS]

ZABEZPIECZENIA

ZASILANIE AWARYJNE SYSTEMÓW ELEKTRONICZNYCH

23 **Zasilanie awaryjne elektronicznych systemów zabezpieczeń**
[SATEL]

44 **OD WYDAWCY**

Dwumiesięcznik Ochrona i Bezpieczeństwo powstaje we współpracy z

Forum Służby Więziennej

Instytut Bezpieczeństwa Pożarowego NODEX Niezależny Ośrodek Doradztwa i Ekspertyz

PISA

20 SPIN: Jubileuszowe Spotkanie Projektantów Instalacji Niskoprądowych!

W dniach 28–29 września 2022 r w Hotelu Bania**** Thermal & SKI odbędzie się dwudziesta, południowa edycja Spotkania Projektantów Instalacji Niskoprądowych. Na Uczestników czeka wiele atrakcji oraz nowości w formule wydarzenia.

Przez 20 lat SPIN stał się unikalną, biznesową platformą wymiany kontaktów i opinii na temat projektowania w branży instalacji niskoprądowych. Jest istotnym punktem w historii rozwoju rynku, ekspansji technologii i innowacji w projektowaniu i integracji systemów. Lockus jako organizator z przyjemnością obserwuje progres i dynamikę rozwoju rynku. Jednocześnie będąc stałym partnerem biznesowym dla firm z branży, wdraża rozwiązania i usługi będące odpowiedzią na nowe oczekiwania i rosnące potrzeby rynku.

Tematyka SPIN obejmuje szeroki wachlarz specjalizacji z branży niskich prądów: od systemów sygnalizacji pożarowej, nowoczesnych systemów CCTV, systemów kontroli dostępu, systemów DSO, systemów zarządzania budynkiem, poprzez systemy zasilania gwarantowanego, rozwiązania Data Center, systemy parkingowe, po profesjonalne rozwiązania sieciowe, multimedialne i integrację systemów.

W programie jubileuszowego spotkania nie zabraknie wielu merytorycznych wykładów, praktycznych warsztatów, a także prezentacji eksperckiej oraz czasu na rozmowy z w strefie biznesowej. Przewidziano także czas na integrację w kompleksie basenów termalnych w Hotelu Bania oraz uroczystą kolację z atrakcjami.

Edycja południowa dedykowana jest dla projektantów z południowej lub centralnej Polski. Rejestracja na wydarzenie odbywa się za pośrednictwem formularza zamieszczonego na stronie www.spin.lockus.pl

Wśród pierwszych Wystawców, którzy potwierdzili swoją obecność znajdują się następujące firmy: 2N, Aco, BKT Elektronik, Dahua Technology, Dormakaba, Hikvision, Impakt wraz z PowerWalker, Intelek/Solarix, Molex, NSS/BCS, Pawlaki Pro Audio, Poltel Telecom wraz z Corning Optical Communications, RCS Engineering, Roger, Romi, Salto Systems, Tommex, Unicard, Zpas.

Szczegółowe informacje na temat nadchodzącej edycji można znaleźć na:

- **spin.lockus.pl**
- **www.facebook.com/SPINiSPINExtra**
- **https://pl.linkedin.com/showcase/spotkanie-projektantów-instalacji-niskoprądowych**

Z okazji Jubileuszu 10-lecia firmy CIAS Sp. z o.o. nasza redakcja została zaproszona do Pałacu Mała Wieś, który położony jest pod Warszawą pośród przepięknych ogrodów i parku na terenie rezerwatu Modrzewina. Był to wspaniale spędzony czas w gronie najbliższych przyjaciół i partnerów CIAS Polska, którzy ze swojej strony zapewnili zaproszonym gościom wyjątkową atmosferę i niezapomniane wrażenia. Zespół Pałacowy Mała Wieś okazał się wyjątkowo urokliwy, pogoda wspaniale dopisywała a całości dopełniły kulinarne doznania na najwyższym poziomie. Pragniemy jeszcze raz podziękować za wspólnie spędzone chwile, przywołać dobre wspomnienia oraz pogratulować Jubileuszu, życząc dalszych długich lat działalności w branży oraz wielu sukcesów.

JAK KOMPLEKSOWO DBAĆ O BEZPIECZEŃSTWO W BRANŻY PRZEMYSŁOWEJ?

Obiekty przemysłowe mają priorytetowe znaczenie dla gospodarek państw. Kluczowe zatem jest odpowiednie podejście do projektowania systemów dozoru obiektów przemysłowych, zarówno w kontekście ochrony perymetrycznej, jak i właściwego zabezpieczenia linii produkcyjnych. Tak szerokie spektrum potrzeb wymaga wdrożenia kompleksowych rozwiązań z zakresu monitoringu wizyjnego, technologii audio i analityki.

W branży przemysłowej wszystkie elementy muszą idealnie do siebie pasować, by zminimalizować wystąpienie incydentu, który mógłby spowodować, np. spadek wydajności linii produkcyjnej. Podobnie jest z sieciowymi systemami dozoru wizyjnego, gdzie komplementarność wdrażanych rozwiązań pozwala na szybsze przekazywanie informacji między urządzeniami – tym samym wpływając na stopień ochrony danego obiektu.

Zakłady przemysłowe to przeważnie duże kompleksy, wymagające stałej ochrony, także pod kątem bezpieczeństwa pracowników przebywających na terenie produkcyjnym. Dlatego też wdrożenie zintegrowanego systemu bezpieczeństwa w modelu *end-to-end* to wartość dodana dla przedsiębiorstwa z różnych powodów – nie tylko pod względem kompleksowej ochrony całego obiektu, ale także na potrzeby wyciągania przyszłościowych wniosków poprawiających bezpieczeństwo i optymalizujących prace całego obiektu.

Pełna ochrona zakładu przemysłowego

Wyobrażając sobie obiekt przemysłowy mamy na myśli ogromną halę produkcyjną z przestronnym, przynależącym do niego otoczeniem zewnętrznym. By skutecznie monitorować tak rozbudowaną przestrzeń, pomocne będą rozwiązania, łączące możliwości dozoru wizyjnego, IP audio i kontroli dostępu. Tak rozbudowany system będzie szczególnie cenny w przypadku np. nieautoryzowanego wtargnięcia intruza na teren zakładu. Wówczas kamery przystosowane do wykrywania podejrzanych zachowań i podążania za obiektem w ruchu są w stanie wykryć niepowołaną osobę. Dzięki zainstalowanym w urządzeniu funkcjom analitycznym kamera może wysłać odpowiedni komunikat pracownikom ochrony budynku. Dodatkowo urządzenia wyposażone w systemy IP audio, umożliwiają emitowanie komunikatów, których zadaniem jest odstraszenie intruza. Uzupełnieniem będą również rozwiązania kontroli dostępu – zezwalające na dostęp do wybranych stref tylko osobom do tego upoważnionym.

Bezpieczeństwo pracowników

Kamery umieszczone w całym zakładzie, mogą wychwycić potencjalne zagrożenia dla osób przebywających na terenie obiektu. Przykładowo kamery termowizyjne są w stanie wykryć niebezpieczne wzrosty temperatury, np. na linii produkcyjnej, a następnie przekazać zebrane dane do zintegrowanego systemu powiadomień audio, dzięki któremu zostanie wyemitowane ostrzeżenie. Zautomatyzowane systemy pozwalają również na stworzenie tzw. niewidzialnych linii, czyli stref, których przekroczenie mogłoby stanowić bezpośrednie zagrożenie dla zdrowia pracowników. Połączone systemy audio/wideo są w stanie wykryć obecność osoby przebywającej w strefie zagrożenia, a następnie wysłać odpowiedni komunikat nakazujący opuszczenie obszaru.

Połączenie systemów dozoru wizyjnego z technologiami IP audio może również być pomocne przy weryfikacji tego, czy pracownicy stosują odpowiednie zabezpieczenia podczas przebywania na terenie zakładu, np. prawidłowe noszenie kasków. Kamera jest w stanie wychwycić osobę, która nie stosuje należytych środków ochrony osobistej, a następnie przekazać tę informację do systemu powiadomień audio.

Optymalizacja procesów i wyciąganie wniosków dzięki analityce

Dzięki integracji różnych rozwiązań sieciowych możliwa jest także analiza procesów zachodzących w zakładzie, co pozwala na zwiększenie wydajności operacyjnej firmy oraz zoptymalizowanie prac wykonywanych na terenie zakładu. Umieszczenie kamer w strategicznych miejscach, np. nieopodal linii produkcyjnej, może mieć kluczowe znaczenie w weryfikacji tego, czy cały proces przebiegł zgodnie z określonymi procedurami. Dane pozyskane z monitoringu są na bieżąco, nieprzerwanie analizowane w kamerze. Zastosowane algorytmy są w stanie wychwycić ewentualne błędy czy awarie maszyn. Zebrane informacje są przekazywane do odpowiedniego oprogramowania do zarządzania materiałem wizyjnym, dzięki czemu jego operator, ma możliwość bezpośredniego wglądu do sytuacji i zasygnalizowania wystąpienia problemu.

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

oraz na profilu
www.facebook.com/AxisCommunicationsPoland

TARGI POLSECURE 2022 – TO BYŁ UDANY DEBIUT

„Bardzo dziękuję przedstawicielom różnych służb, za to że jesteśmy na tych targach wszyscy razem. To był jeden z elementów sukcesu tego wydarzenia” – tak Międzynarodowe Targi Policji i Bezpieczeństwa Publicznego podsumował, podczas swojego wystąpienia na gali wręczenia nagród kończącej wystawę I Zastępca Komendanta Głównego Policji nadinspektor Dariusz Augustyniak. Wydarzenie było współorganizowane przez Komendę Główną Policji. Partnerem strategicznym Targów była GRUPA WB.

Nadinspektor podkreślił zaangażowanie w realizację przedsięwzięcia zarówno służb podległych Ministerstwu Spraw Wewnętrznych i Administracji, jak również innych instytucji reprezentowanych w Komitecie Honorowym i Radzie Programowej POLSECURE. Taka opinia jest szczególnie ważna podczas debiutu wydarzenia targowego, który zawsze wiąże się z niepewnością, co podkreślali także sami wystawcy.

„Szczerze mówiąc, na samym początku dosyć sceptycznie podchodziliśmy do tej imprezy. Pierwsza edycja jest zawsze ryzykowną inwestycją” – tak udział firmy WORKS 11 podsumowywał prezes zarządu Jakub Bokiewicz – „Targi POLSECURE okazały się jednak bardzo udane. Mieliśmy wielu klientów z kluczowych dla nas instytucji rządowych, co wiązało się z bardzo ciekawymi rozmowami na temat potencjalnej sprzedaży”

Targi rozpoczęły się ceremonią oficjalnego otwarcia, w której udział wzięło wielu znakomitych gości, na czele z Podsekretarzem Stanu w Ministerstwie Spraw Wewnętrznych i Administracji, Bartoszem Grodeckim oraz generalnym inspektorem Jarosławem Szymczykiem, Komendantem Głównym Policji wraz z zastępcami: nadinspektorem Dariuszem Augustyniakiem i nadinspektorem Pawłem Dobrodziejem. Po ceremonii Goście, w tym delegacje zagraniczne odwiedziły ekspozycję targową.

Merytoryczna strona Targów POLSECURE – Międzynarodowa Konferencja Policji

W pierwszym dniu Konferencji w całości poświęconemu cyberbezpieczeństwu przedstawiciele najważniejszych międzynarodowych organizacji dotyczących bezpieczeństwa publicznego podzielili się swoją wiedzą z polską policją. W panelu dyskusyjnym pod nazwą „Obecne zagrożenia i trendy cyberprzestępczości” brali udział Craig Jones z INTERPOLU,

Edvardas Sileris z EUROPOLU, Craig Wolf – z US Secret Service, Carsten Meywirth z niemieckiego BKA i Elvis Chan z FBI.

Drugi dzień konferencji poświęcony był modernizacji i rozwojowi. Przedstawiciele policji, straży pożarnej oraz służb więziennych dyskutowali o nowych mundurach, asortymencie i wpływie postrzegania na pracę policji i innych służb bezpieczeństwa publicznego.

Trzeci dzień był „Dniem samorządowym". Uczestnicy konferencji dyskutowali m. in. o zasadach bezpieczeństwa na wypadek zagrożenia życia, czy też o monitoringu w przestrzeni publicznej. Panel rozpoczął prezydent Kielc, Bogdan Wenta. Wspomniał on m. in. o tym jak łatwo jest zaburzyć poczucie bezpieczeństwa publicznego, np. groźbą mailową, ale też jak ważny jest skuteczny system szybkiego reagowania na wszelkiego rodzaju zagrożenia, bez względu na ich skalę i rodzaj.

Pokazy dynamiczne – ważny element targów policyjnych

Pokazy: kontrterrorystów z użyciem psa bojowego, musztry paradnej, psów policyjnych, ratownictwa motocyklowego, czy prezentacje najnowszych dronów można było oglądać przez trzy dni w Targach Kielce. Dynamiczne show przygotowane przez Centralny Pododdział Kontrterrorystów Policji „BOA" wzbudził duże zainteresowanie widzów.

Partner strategiczny Targów POLSECURE z premierą i umową

Pierwszego dnia targów Grupa WB zaprezentowała prototyp osobistego, bezzałogowego czterowirnikowca. Najnowszy *bezpilotowiec* (bsp), opracowany przez inżynierów spółki Flytronic (wchodzącej w skład Grupy WB), jest konstrukcja wielozadaniową mogącą wspierać zarówno żołnierzy w walce jak i wspierać rozbudowane systemy monitoringu.

POLSECURE pod znakiem nowych barw radiowozów

Projekt tego, jak mają wyglądać nowe auta policyjne można było zobaczyć już wielokrotnie na różnych pokazach. Od teraz będzie je można zobaczyć także na ulicach polskich miast. Oficjalna premiera odbyła się w drugim dniu Międzynarodowych Targów Policji i Bezpieczeństwa Publicznego.

Jak podkreślił podczas prezentacji nowych radiowozów nadinspektor Dariusz Augustyniak, I zastępca Komendanta Głównego Policji, planowana zamiana wyglądu pojazdów jest podyktowana przede wszystkim dążeniem do ich jak najlepszej widoczności.

Gala wręczenia nagród na koniec POLSECURE

Międzynarodowe Targi Policji i Bezpieczeństwa Publicznego zostały zakończone uroczystym wręczeniem nagród dla najlepszych produktów.

Wręczone zostały także nagrody TOP DESIGN za najbardziej efektowne stoiska. I Zastępca Komendanta Głównego Policji nadinspektor Dariusz Augustyniak wręczył również wyróżnienie specjalne KOMENDANTA GŁÓWNEGO POLICJI.

Więcej szczegółowych informacji na stronie:
www.targikielce.pl/polsecure

Międzynarodowe Targi Zabezpieczeń Securex to od lat jedno z najważniejszych wydarzeń biznesowych skierowanych dla branży zabezpieczeń. Różnorodność ekspozycji w tym roku zapewniły firmy, które oferowały zwiedzającym szeroki wachlarz produktów, usług i innowacyjnych rozwiązań.

Najbardziej innowacyjne rozwiązania zostały nagrodzone **Nagrodą Złotego Medalu Targów Securex** oraz **Złotego Medalu Poznań Media Expo**. Zachęcamy do zapoznania się z listą laureatów: https://www.securex.pl/pl/aktualnosci/poznaj-laureatow-zlotego-medalu-targow-securex-oraz-pme-2022/

Swoje **jubileusze** świętowały także na targach: Polska Izba Radiodyfuzji Cyfrowej – 20-lecie; firma C&C Partners – 30-lecie; Polski Związek Pracodawców Ochrona – 30-lecie.

Targom Securex towarzyszyła bogata oferta konferencji, warsztatów i debat.

Podczas Targów SECUREX odbyło się również **spotkanie z Piotrem Niemczykiem** – komentatorem i publicystą, b. zastępcą Dyrektora Wywiadu UOP, b. Wiceministrem Gospodarki oraz autorem książek „Krótki kurs szpiegowania", „Szósta rano. Kto puka? Jak ojczyzna Solidarności zmienia się w państwo policyjne", „Pogarda. Dlaczego rośnie liczba przestępstw z nienawiści w Polsce?". Niemczyk odniósł się w jego trakcie do obecnej sytuacji wojny w Ukrainie.

Każdego dnia targowego **Krajowe Stowarzyszenie Ochrony Informacji Niejawnych** oraz **Sto-**

warzyszenie Wspierania Bezpieczeństwa Narodowego oferowały zwiedzającym konsultacje w zakresie ochrony informacji niejawnych, biznesowych, danych osobowych, bezpieczeństwa obiektów oraz cyberbezpieczeństwa. Więcej informacji na ten temat: https://www.securex.pl/pl/aktualnosci/poznaj-program-wydarzen-ksoin-i-swbn-w-trakcie-targow-securex/

Serdecznie dziękujemy za uczestnictwo w tegorocznej edycji i zachęcamy do udziału w Targach wiosną 2024 roku.

Zespół Targów Securex

Reklama

CARRIER

II OGÓLNOPOLSKIE WARSZTATY REAGOWANIE NA ZAMACHY – DOBRE PRAKTYKI I REKOMENDACJE

W dniach 24–25 maja odbyły się II-gie ogólnopolskie warsztaty Reagowanie na Zamachy – Dobre Praktyki i Rekomendacje. To kolejna impreza organizowana dzięki współpracy Aritech i Safety Project. Współpraca ta ma na celu promocję świadomości o zagrożeniach oraz wiedzy o metodach prewencji i usuwaniu skutków zdarzeń o naturze terrorystycznej czy skutków katastrof naturalnych. Dwa dni intensywnego szkolenia, ćwiczeń praktycznych, dyskusji i wymiany doświadczeń pomiędzy uczestnikami oraz zaproszonymi ekspertami dały impuls do działania oraz pozwoliły poczuć choć namiastkę realnych zdarzeń w trakcie przygotowanych symulacji i ćwiczeń. Głównymi tematami były zagadnienia przygotowania obiektów i organizacji do skutecznego reagowania na zdarzenia z szerokiego spektrum zagrożeń np.: przyjęcie komunikatu o zagrożeniu, masowy zabójca, materiały wybuchowe, pierwsza pomoc oraz wykorzystanie zabezpieczeń technicznych itd. Możliwość spotkania i wymiany doświadczeń praktyków odpowiedzialnych za przygotowanie obiektów z ratownikami i specjalistami-weteranami służb antyterrorystycznych umożliwiło nowe spojrzenie na tematykę warsztatów bez konieczności zdobywania własnego doświadczenia w traumatycznych okolicznościach. Już dzisiaj zapraszamy na kongres Safe Place, który odbędzie się 17–19.10.2022 oraz następne edycje warsztatów.

pl.firesecurityproducts.com

Aritech jest globalną marką firmy Carrier Fire & Security reprezentującą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferujemy zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, wideo i wykrywania pożaru.

AMBIENT SYSTEM

NOWE GŁOŚNIKI W NASZEJ OFERCIE!

Z dumą informujemy, iż NOWE GŁOŚNIKI ABT-T1410, ABT-T2015 wzbogaciły nasze portfolio głośników pożarowych.

Charakterystyka:

- Doskonała zrozumiałość mowy
- Środowisko pracy A, B, C
- Wysoki stopień ochrony przed pyłem i wilgocią (IP66)
- Zabezpieczenie linii głośnikowej przed zwarciem lub przerwą
- Montaż na ścianie i suficie
- Dwa wejścia kablowe izolowane dławnicami
- Pełna zgodność z normą PN-EN 54-24
- Certyfikat zgodności CNBOP: 1438-CPR-0801
- Zabezpieczenia termiczne zgodne z normą BS5839-8

Zastosowanie:

- Perony kolejowe
- Parkingi naziemne i podziemne
- Hale magazynowe
- Parki
- Szkoły i boiska

ROGER

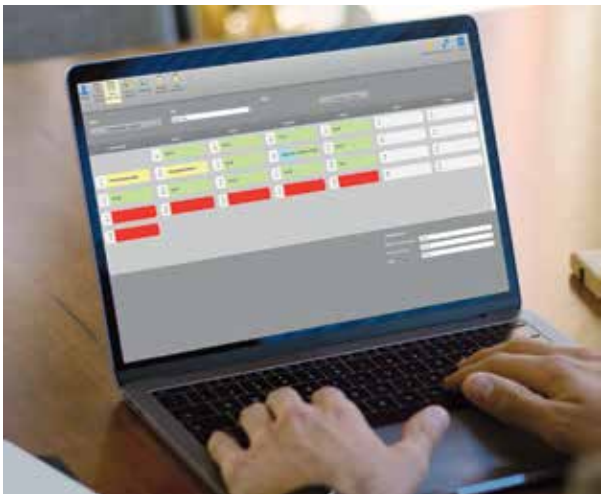
NOWA EDYCJA PROGRAMU RCP MASTER DO ANALIZY I ROZLICZANIA CZASU PRACY

Program RCP Master (Roger) przeznaczony do analizy i rozliczania czasu pracy jest dostępny na rynku od prawie 15 lat. W tym czasie ukazały się 3 edycje tego programu. Na początku bieżącego roku została wydana jego kolejna, czwarta już wersja.

RCP Master 4 udostępnia wszystkie dostępne wcześniej funkcjonalności, które potwierdziły swoją wartość w tysiącach wdrożonych z sukcesem instalacji oraz oferuje szereg nowych możliwości dostosowanych do wymogów dzisiejszego rynku pracy.

Nowa edycja programu zawiera m.in. moduł RCP Master 4 Web, który umożliwia pracownikom dostęp do wybranych funkcji systemu rejestracji czasu pracy (RCP) za pośrednictwem przeglądarki internetowej. Pracownik korzystający z RCP Master 4 Web może zapoznać się z aktualnym stanem wypracowanego czasu pracy, przejrzeć rejestr zdarzeń, złożyć wniosek o urlop lub zgłosić innego rodzaju absencję bez konieczności kontaktu z działem kadr. Ponadto, moduł RCP Master 4 Web umożliwia zdalną rejestrację zdarzeń RCP, w tym rejestrację pracy zdalnej.

RCP Master 4 Web zapewnia również zestaw funkcji przeznaczonych dla przełożonych różnego szczebla (kierownicy, brygadziści, liderzy zespołów itp.), którzy zyskują w ten sposób wygodny i szybki sposób wglądu w czas pracy osób funkcjonujących w ramach zarządzanej grupy pracowniczej.



Tak jak poprzednie wersje programu, RCP Master 4 może pracować niezależnie lub stanowić integralną część systemu kontroli dostępu RACS 4 lub 5. Kontynuowany jest elastyczny i korzystny system licencjonowania, który umożliwia dobór licencji w zależności od wielkości i potrzeb firmy. RCP Master 4 jest w pełni kompatybilny z RCP Master 3, co umożliwia szybką i wygodną migrację do nowszej wersji programu.

C&C

PRZEMYSŁOWE STACJE INTERKOMOWE SIP – TRWAŁE ROZWIĄZANIE KOMUNIKACYJNE

Koncentrując się na najwyższym poziomie bezpieczeństwa, prostej obsłudze i przyszłej skalowalności, przemysłowe stacje IP z serii EE 7000H od Commend są przeznaczone do komunikacji w trudnych warunkach.

Wersje stacji serii EE 7000H zapewniają dokładnie to, czego wymagają zarówno użytkownicy, jak i lokalne przepisy.

Oparta na wytrzymałej, odpornej na korozję i lekkiej obudowie z poliwęglanu seria EE 7000H umożliwia prosty i szybki montaż, eliminuje kosztowne rutynowe serwisowanie i znacząco obniża koszty konserwacji.

Dodatkowo certyfikat IP66 i szeroki dopuszczalny zakres temperatur sprawia, że przemysłowe stacje interkomowe są doskonałym wyborem do szerokiej gamy zastosowań. Dzięki wysokiej jakości mikrofonom i dźwiękowi 16 kHz eHD Voice, seria EE 7000H zapewnia najwyższą zrozumiałość mowy.

Nawet w bardzo hałaśliwym otoczeniu dwa potężne wzmacniacze wbudowanego głośnika i podłączany głośnik PA zapewniają krystalicznie czysty dźwięk. Ponadto mikrofon i funkcja IVC (Intelligent Volume Control) pozwalają na automatyczne dostosowanie głośności do hałasu otoczenia – nawet podczas odtwarzania.

Ponieważ urządzenia obsługują zarówno połączenia IoIP, jak i rozwiązania SIP (hybrydowe), stacje można łatwo zintegrować z dowolnym systemem Voice over IP, w tym istniejącym już systemem interkomowym Commend. Wymagany tryb pracy jest wybierany za pomocą oprogramowania konfiguracyjnego.

EWOLUCJA CZY REWOLUCJA?
NOWY ZEWNĘTRZNY SYGNALIZATOR GŁOSOWO-OPTYCZNY TYPU SGO-PGZ3

Wstęp

W ofercie W2 pojawił się nowy sygnalizator, który jest kolejnym przedstawicielem serii zewnętrznych sygnalizatorów głosowo-optycznych. SGO-Pgz3, bo o nim mowa podobnie jak poprzednicy spełnia wymagania norm zharmonizowanych EN 54-3:2001+A1:2002+A2:2006 oraz EN 54-23:2010. Na wyrób przez CNBOP-PIB wydane zostały Certyfikat Stałości Właściwości Użytkowych oraz Świadectwo Dopuszczenia.

Budowa

Sygnalizator SGO-Pgz3 wyglądem przypomina SGO-Pgz2. Posiada on bowiem taką samą obudowę. Jedyną widoczną dla użytkownika różnicą z zewnątrz jest konstrukcja klosza lampy członu optycznego. W SGO-Pgz3 jest ona wykonana z dyfuzorem, co poprawia walory estetyczne (nie widać elementów znajdujących się wewnątrz). Zmiany konstrukcyjne objęły przede wszystkim elektronikę.

W nowym członie optycznym zmienione zostało źródło światła z palnika ksenonowego (SGO-Pgz2) na 4 wysokiej jasności diody LED. Pozwoliło to zwiększyć uzyskiwaną bryłę fotometryczną przy jednoczesnym obniżeniu poboru prądu. Dodatkowo dostępne są różne konfiguracje optyki. Urządzenie występuje w 3 odmianach:

- SGO-Pgz3 – światło czerwone (4 diody), klosz lampy w kolorze czerwonym,
- SGO-Pgz3/śb – światło białe (2 diody), klosz lampy w kolorze białym,
- SGO-Pgz3/śbcz – światło białe i czerwone naprzemiennie (2 czerwone i 2 białe diody), klosz lampy w kolorze białym.

Należy pamiętać, że Świadectwem Dopuszczenia CNBOP-PIB jest objęta jedynie wersja SGO-Pgz3.

Jeśli chodzi o człon akustyczny to jako przetwornik dźwięku zastosowano głośnik 4 Ω o wysokiej efektywności > 90 dB (1W/1m) w szerokim paśmie. W celu uzyskania jak najlepszych parametrów akustycznych w urządzeniu zastosowano wzmacniacz audio pracujący w klasie D z układem wyciszenia stuknięć w głośniku o mocy wyjściowej ok. 20 W RMS 1 kHz. Nowa konstrukcja członu akustycznego pozwoliła poprawić nie tylko poziom dźwięku sygnału alarmowego czy komunikatu, lecz również ich jakość.

Zarówno część optyczna, jak i akustyczna może być synchronizowana (równe błyski lamp oraz odtwarzanie komunikatu w tym samym momencie we wszystkich urządzeniach pracujących w sieci). Może okazać się to istotne i wręcz konieczne w momencie budowania większych sieci sygnalizatorów (np. więcej niż 1 sygnalizator optyczny widoczny z tego samego punktu).

Funkcjonalności

Sygnalizator SGO-Pgz3 został zaprojektowany zupełnie od nowa w taki sposób, żeby był on kompatybilny z innymi urządzeniami W2 dostępnymi na rynku (sygnalizatory wewnętrzne: głosowe SG-Pgw2, SG-Pgw3 oraz sygnalizator głosowo-optyczny SGO-Pgw). Dzięki temu istnieje możliwość rozbudowy już istniejących instalacji o nowe sygnalizatory SGO-Pgz3 bez konieczności zmiany okablowania. Podobnie jak we wspomnianych sygnalizatorach w pokrywie urządzenia znaleźć można:

- zaciski zasilania oraz wyzwalania komunikatów oznaczone jako $+_1$,$+_2$,GND,
- zaciski synchronizacji oznaczone jako S_A, S_B,
- zaciski do podłączenia WSD-1 oznaczone jako D,+,GND,
- złącze microUSB do komunikacji (zmiana ustawień sygnalizatora np. syreny),
- potencjometr do płynnej regulacji poziomu dźwięku.

W zależności od tego, na które zaciski poda się napięcie zasilania, zostanie wyzwolony dany komunikat znajdujący się w pamięci urządzenia ($+_1$ – K1.mp3, $+_2$ – K2.mp3, $+_1$ i $+_2$ – K3.mp3). Umożliwia to zmianę nadawanego komunikatu w trakcie alarmu. Sygnalizator SGO-Pgz3 został wyposażony w blokadę podnapięciową (przy zasilaniu do 16 V DC pobór prądu jest bliski 0 mA), funkcję autoadresowania (brak konieczności wyboru trybu pracy MASTER / SLAVE), magistralę komunikacyjną CAN (kopiowanie pamięci, synchronizacja akustyki oraz optyki) czy funkcję autoaktualizacji (możliwość przekopiowania ustawień z jednego urządzenia do pozostałych pracujących w sieci).

Dodatkowo dla synchronizacji zastosowano zabezpieczenie przed uszkodzeniem (w przypadku uszkodzenia czy problemów z magistralą sygnalizatory zadziałają bez synchronizacji). Nowością jest zastosowanie ogranicznika prądu rozruchowego, który pozwala zmniejszyć wartość amplitudy przebiegu prądu po uruchomieniu sygnalizatora ponad 4x.

Autodiagnostyka

Istotna z punktu widzenia użytkownika może być również autodiagnostyka akustyczna oraz optyczna. Dzięki tym funkcjonalnością możliwe jest szybkie zdiagnozowanie ewentualnych problemów, które mogą wystąpić. Jeśli w urządzeniu brakuje plików lub są one nieprawidłowe sygnalizator będzie generował sygnał o częstotliwości 1 kHz 1s on/1s off. Błąd na wejściu adresującym lub uszkodzenie sygnalizatora spowoduje generowanie sygnału o częstotliwości 2 kHz 0,5s on/0,5 s off. Nowością jest optyczna sygnalizacja błędów podczas kopiowania komunikatów. Pozwala ona wykryć błędy powstałe przy przesyłaniu plików po sieci sygnalizatorów (wykorzystana funkcja autoaktualizacji). Błąd jest wykazywany poprzez szybkie błyski generowane przez lampę. W przypadku, gdy błyski są generowane przez urządzenie z ustawioną opcją autoaktualizacji na 1 oznacza to, że to urządzenie odnotowało sygnał żądania ponownego kopiowania z innego (innych) sygnalizatora-ów pracujących w sieci. Jeśli błyski są generowane przez urządzenie z opcją autoaktualizacji na 0 oznacza to, że nie udało się mu zaktualizować pamięci. Warto podkreślić, że podczas procesu kopiowania lampa nie błyska, słychać jedynie sygnał dźwiękowy. Jeżeli w trakcie kopiowania uruchomi się, któryś z sygnalizatorów oznacza to, że jest on nieprawidłowo podłączony do sieci. Po kopiowaniu odtwarzane są komunikaty zgodnie ze stanem na wejściach adresujących, lampa błyska normalnie. Sam proces w zależności od ilości plików oraz ich wagi może trwać nawet ok. 10 minut. Po kopiowaniu ustawień warto sprawdzić, czy któryś z sygnalizatorów nie zgłasza błędu. Jest to ważne, ponieważ po odłączeniu zasilania pamięć o błędach się kasuje.

Podsumowanie

Jak widać sygnalizator SGO-Pgz3 ma kilka wspólnych cech i funkcjonalności z sygnalizatorami SG-Pgw2, SG-Pgw3, SGO-Pgw. Dzięki temu uzyskano kompatybilność wsteczną pozwalającą na bezproblemowe budowanie układów składających się z tego typu urządzeń. Zastosowanie nowych rozwiązań pozwoliło osiągnąć lepsze parametry techniczne (np. poziom dźwięku na poziomie >100 dB) niż wspomniane sygnalizatory. W projekcie zawarto sporo nowości takich jak: ogranicznik prądu rozruchowego, optyczna sygnalizacja błędów przy kopiowaniu komunikatów, czy wzmacniacz audio pracujący w klasie D. Nowe rozwiązania pozwoliły uzyskać bardzo dobre parametry, jeśli chodzi o poziom oraz jakość dźwięku, jak i również wielkość bryły fotometrycznej przy jednoczesnym stosunkowo niewielkim poborze mocy z zasilacza.

Reklama

REJESTRACJA OBRAZU W TELEWIZJI DOZOROWEJ CCTV

Telewizja przemysłowa CCTV (ang. Closed Circuit TeleVision) nazywana obecnie częściej monitoringiem wizyjnym, jest narzędziem umożliwiającym obserwację i rejestrację obrazu za pomocą kamer znajdujących się w pewnej odległości od obiektu. W systemach dozoru wciąż obecne są trzy rodzaje monitoringów wizyjnych – analogowy, hybrydowy oraz cyfrowy (czyli IP).

Damian Żabicki

Rodzaje monitoringu wizyjnego

Najstarsza telewizja przemysłowa oparta była na systemie analogowym. Miała swoje ograniczenia – pozwalała na realizację podglądu wyłącznie w obrębie sieci lokalnej zbudowanej na kablach koncentrycznych, łączących indywidualnie kamery z rejestratorem. Obraz zapisywany był w rozdzielczości PAL/NTSC – czyli maksymalnie ok. 768×576 pikseli. Choć nie jest to wysoka jakość, tego typu systemy wciąż funkcjonują w wielu obiektach komercyjnych i przemysłowych.

Nieco bardziej zaawansowane są systemy hybrydowe. Działają one w oparciu o hybrydowe rejestratory lub serwery wizyjne IP, umożliwiające łączenie kamer analogowych z urządzeniami cyfrowymi IP i korzystające z ich funkcjonalności. W praktyce urządzenia hybrydowe po prostu konwertują sygnał analogowy na cyfrowy i umożliwiają jego cyfrowy zapis lub pozwalają na zdalny podgląd.

Najnowocześniejszym rozwiązaniem w systemach dozoru wizyjnego jest monitoring IP. Wykorzystuje on protokół internetowy IP, pozwa-

lający na tworzenie dużych, otwartych na rozbudowę systemów przy wykorzystaniu istniejącej infrastruktury sieci LAN.

Zalet systemu IP, w stosunku do poprzedników, jest wiele. Przede wszystkim nie ma konieczności łączenia każdej kamery bezpośrednio z rejestratorem. To powoduje, że monitoring IP jest bardziej elastyczny a do tego umożliwia rozproszenie urządzeń działających w obrębie wykorzystywanej sieci i – co za tym idzie – prostą i szybką rozbudowę systemu.

Walorem jest także jakość obrazu rejestrowanego za pośrednictwem kamer megapixelowych. W tym wypadku użytkownika ogranicza właściwie jedynie wielkość matrycy i przetwornika. Powszechnie stosowane są już kamery o rozdzielczościach HD (1.0 Mpx – 1280x 720) czy Full HD (2.0 Mpx– 1920–1080). Co więcej, na rynku znaleźć można także kamery o rozdzielczościach powyżej 3.0 Mpx, które pozwalają na dokonywanie zapisu o bardzo wysokiej jakości. Tego typu urządzenia stosowane są n.in. do obserwacji obiektów magazynowych.

Składowe systemu IP

W skład systemu telewizji dozorowej CCV opartej na protokole IP, wchodzą kamery IP, rejestratory IP, switch i router.

Kamery IP nagrywają, podobnie jak kamery analogowe, jednak wyposażone są także w funkcje małego komputera. Pozwalają na transmisję obrazu w czasie rzeczywistym za pomocą sieci IP. Mogą też, dzięki wbudowanym serwerom WWW, FTP, pracować niezależnie od komputera, co umożliwia montaż w dowolnym miejscu, pod warunkiem, że ma ono dostęp do wifi.

Rejestrator sieciowy IP (ang. Network Video Recorder – NVR) służy do obsługi i zarządzania systemami monitoringu IP. To samodzielne urządzenie, które przechwytuje obraz z kamer IP pracujących w obrębie określonej sieci LAN. Rejestratory sieciowe pozwalają na podgląd i zapis obrazu a także na jego archiwizację na dyskach twardych i w chmurze. Mogą obsługiwać od 4 aż do kilkudziesięciu kamer jednocześnie, co pozwala na ich zastosowanie także w dużych systemach.

Z kolei switch przekazuje dane między elementami sieci z doborem portu przełącznika, na który dane są przekazywane. To podstawowe urządzenie służące do połączenia kilku kamer z rejestratorem i zapewniające prawidłowe funkcjonowanie systemu monitoringu w sieci lokalnej.

I w końcu router, którego zadaniem jest łączenie różnych sieci komputerowych. To swoisty węzeł komunikacyjny. Zastosowanie routera pozwala na udostępnienie obrazu na zewnątrz, za pośrednictwem Internetu a także na zdalny dostęp i zarządzanie monitoringiem, bez względu na miejsce, w którym znajduje się użytkownik. Wystarczy, że ma dostęp do przeglądarki internetowej lub aplikacji mobilnej.

Rodzaje kamer IP

Na rynku oferowana jest cała gama kamer IP. Jak w ich gąszczu znaleźć odpowiednią? Oczywiście, trzeba wziąć pod uwagę własne potrzeby, a także wymogi zabezpieczanego obiektu. Przydatne okaże się również zaznajomienie z rodzajami kamer i ich funkcjami.

Kamery tubowe (bullet) to urządzenia cieszące się największą popularnością w systemach dozoru obiektów. Wyposażone są w stały korpus oraz stopę montażową. Kierunek i zakres obserwowanego pola jest pokłosiem ich kształtu. Najczęściej stosowane są w miejscach, w których istnieje konieczność (lub takie są oczekiwania właściciela obiektu), aby nie rzucać się w oczy i nie odstraszać zawczasu intruzów.

Kamery kopułkowe (dome) zbudowane są w sposób umożliwiający dyskretną obserwację. Intruz nie wie, gdzie skierowany jest obiektyw. Dodatkowo urządzenia te posiadają zwykle wandaloodporną konstrukcję. Są dedykowane do montażu sufitowego, a zatem cechuje je większy kąt widzenia, niż ma to miejsce w przypadku kamer tubowych.

W tej kategorii można spotkać modele z szerokokątnym obiektywem – tzw. rybim okiem. Pozwala on na obserwację pola o zakresie 180 stopni. Dzięki temu często zamiast kilku, wystarczy zastosowanie jednej kamery. Najczęściej ten

typ kamer instalowany jest w szkołach, centrach handlowych czy na halach produkcyjnych.

Kolejny typ kamer to kamery obrotowe (z ang. Pan Tilt – PT). Pod względem technologicznym są to najbardziej zaawansowane urządzenia spośród kamer stosowanych w monitoringu wizyjnym. Umożliwiają zdalne sterowanie obiektywem i obrotem głowicy we wszystkich kierunkach.

Kryteria doboru kamer do CCTV

Decydując się na zakup kamer do monitoringu wizyjnego, trzeba zacząć od określenia miejsca montażu. W zależności od tego, jak długo w ciągu dnia będą pracować i w jakich warunkach, należy przewidzieć konieczność wybrania właściwego współczynnika ochrony mechanicznej. Jeśli bowiem kamera będzie narażona na uszkodzenia mechaniczne, można rozważyć zakup takiej, która wyposażona została w wandaloodporną obudowę.

Istotna jest także ochrona urządzenia przed niekorzystnymi czynnikami atmosferycznymi. To kryterium dotyczy zwłaszcza kamer zewnętrznych, które poddawane być mogą opadom deszczu czy śniegu.

Niektóre urządzenia przeznaczone są do pracy ciągłej, czyli przez całą dobę 7 dni w tygodniu. Aby rejestracja obrazu była wtedy możliwa, kamera powinna posiadać oświetlenie nocne. Najczęściej są to diody IR, emitujące zakres fal podczerwonych. Aby kamery wyposażone w diody IR działały poprawnie, muszą mieć mechaniczny filtr IR-Cut odcinający światło z diod w ciągu dnia.

Obiektywy

Istotnym elementem kamer używanych w systemach monitoringu wizyjnego, są obiektywy, odpowiadające za tworzenie obrazu oraz jego transmisję. Kluczowe parametry obiektów to ich ogniskowa (rozumiana jako odległość, w jakiej od centrum optycznego obiektu powstaje jego obraz), przesłona, liczba aperturowa obiektywu (tzw. jasność obiektywu), głębia ostrości, liczba transmisyjna obiektywu, rozdzielczość, ostrość, kontrastowość.

Obiektywy mogą być mini, stałoogniskowe, manualne i obiektywy auto iris.

Rejestratory cyfrowe

Urządzenia pozwalające na nagrywanie wideo w formacie cyfrowym to rejestratory cyfrowe. Zapis obrazu następuje w formacie cyfrowym na dyskach twardych lub innych mediach. Najnowsze rejestratory cyfrowe pozwalają na budowę monitoringu w oparciu o siatkę kamer. Obrazy i dźwięki mogą być przechowywane na popularnych nośnikach takich jak CD, DVD lub urządzeniach z wejściem USB. Z kolei podgląd i archiwizacja zdarzeń jest możliwa za sprawą wykorzystania sieci LAN, WAN lub za pośrednictwem Internetu.

Oczywiście rejestratory, podobnie jak kamery, mogą być także analogowe i hybrydowe. Zaletą analogowych jest bez wątpienia kompatybilność ze wszystkimi producentami kamer analogowych. Walorem jest też to, że filmy zajmują małą część dysku nagrań.

I w końcu rejestratory skierowane dla kamer sieciowych IP. W niektórych modelach znaleźć można wbudowany switch PoE, pozwalający na zasilanie kamer z komputera.

Kamery hybrydowe obsługują technologię kamer IP z kamerami analogowymi. Mogą mieć 4, 8 i 24 kanały. Dostępne są także rejestratory trybrydowe, obsługujące 3 rodzaje technologii – kamer analogowych, HD-CVI i AHD.

Wybierając rejestrator do CCTV należy wziąć pod uwagę ilość obsługiwanych kamer (najczęściej istnieje możliwość podłączenia 4,18 lub 16 kamer). Warto zawczasu pomyśleć o tym, czy w przyszłości system ten nie będzie rozbudowywany.

Istotny jest także format kompresji obrazu – np. MPEG-4, MJPEG oraz H.265 i H.264 (najlepszy).

Prędkość nagrywania to kolejne kryterium doboru. Ilość klatek na sekundę jest uzależniona od rozdzielczości. Wybór uwzględniać powinien przeznaczenie monitoringu. Przydatne są także dodatkowe funkcje, takie jak detekcja ruchu, możliwość podglądu przez sieć LAN, port USB, wyjście VGA, harmonogram, a także szereg trybów zapisu (m.in. wg timera, praca ciągła, z detekcji ruchu czy też z wyjść alarmowych)..

Podsumowanie

Systemy telewizji dozorowej CCTV są bardzo ważnym elementem systemów zabezpieczenia życia i mienia. Niezwykle istotna w tym względzie jest rejestracja obrazu, która – aby zapis z urządzenia pozwalał na identyfikację intruza – powinna być oparta o kamerę i rejestrator o najlepszej jakości zapisu. Zarejestrowany obraz powinien być czytelny i szczegółowy. Może być zapisany w kolorach czarnym i białym, może też stać się kolorowym zapisem.

Najważniejsze kwestie, które należy rozstrzygnąć przed wyborem rejestratora dotyczą szczegółowości zapisu – czy ważne są detale, czy tylko ogólny obraz, funkcjonalności sprzętu – czy posiada podstawowe czy rozszerzone oprogramowanie oraz ilość kamer podłączonych do rejestratora – od tego zależy, jaką powinien mieć moc. ■

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

RACS 5 v2

Polski system kontroli dostępu klasy *Enterprise*

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

roger

Intelligence for Building

NOWOCZESNE SYSTEMY PARKINGOWE I OTWIERANIA SZLABANÓW

Automatyczne rozpoznawanie tablic rejestracyjnych przy wjazdach na parkingi czy autostrady to jedno z najbardziej dynamicznie rozwijających się rozwiązań w zakresie automatycznego sterowania ruchem. Systemy „czytające" tablice rejestracyjne pojazdów znacznie usprawniają ruch poprzez skrócenie czasu obsługi pojedynczego pojazdu opuszczającego parking czy przejeżdżającego bramki autostradowe. W takich rozwiązaniach eliminuje się ręczną obsługę związaną z np. opłatami czy koniecznością zeskanowania biletu przy szlabanie.

Robert Gabrysiak

Sposób działania systemu polega na tym, że po odczytaniu przez odpowiednią kamerę tablica rejestracyjna porównywana jest z bazą danych i w zależności od wyniku szlaban zostaje otwarty lub wywołane jest inne zdarzenie. W taki lub podobny sposób działa większość systemów otwierania szlabanów.

Systemy identyfikacji tablic rejestracyjnych znane są też pod oznaczeniami SITR (System identyfikacji tablic rejestracyjnych), ANPR (Automatic number plate recognition) lub LPR (License Plate Recognition). Skuteczne działanie takiego systemu zależy od rodzaju i usytuowania kamery, silnika sterującego szlabanem, oświetlenia, stopnia zabrudzenia tablic rejestracyjnych czy też od prędkości przejeżdżających pojazdów – co ma szczególne znaczenie przy dużym natężeniu ruchu. Kompletny system LPR (czy ANPR) składa się z połączonych w sieci następujących urządzeń:

- Kamery IP z funkcją czytania tablic,
- Serwera z odpowiednim oprogramowaniem,
- Sterowników szlabanów lub innych urządzeń.

Kamera czytająca tablicę, wysyła zarejestrowany obraz do serwera, gdzie poddawany jest on analizie, na podstawie której następuje odczyt numerów rejestracyjnych. Zdjęcie numerów rejestracyjnych może być zapisane na serwerze i zostać wykorzystane do innych celów np. do porównania z bazą numerów rejestracyjnych samochodów skradzionych. Do oprogramowania systemu mamy dostęp z dowolnego urządzenia posiadającego przeglądarkę internetową. Należy pamiętać, że oprogramowanie jest wielopoziomowe zatem różni użytkownicy systemu mogą posiadać różne uprawnienia. Systemy odczytu rejestracji pojazdów charakteryzują się możliwością realizowania bardzo wielu funkcji i tylko od właściciela systemu zależy, które z nich będzie wykorzystywał. Funkcjami tymi są:

- Wspomniane powyżej – alarmowanie o pojazdach skradzionych/poszukiwanych,
- Otwieranie szlabanu dla wszystkich pojazdów lub z pominięciem pojazdów z „czarnej listy" (czyli listy stworzonej przez zarządcę systemu na której znajdują się numery pojazdów, dla których wjazd jest zabroniony),
- Obsługa wielu kamer,
- Rejestracja czasu parkowania,
- Zliczanie wjazdów i wyjazdów,
- W przypadku dużych parkingów możliwość uruchomienia funkcji odnalezienia pojazdu (find my car),
- Klasyfikowanie pojazdów wg ilości wizyt, czasu pobytu czy choćby pory dnia,
- Klasyfikowanie wg lokalizacji z możliwością wizualizacji na mapie Polski,
- Harmonogramowanie wizyt – czyli ustawianie dostępu do parkingu wg określonego harmonogramu (taka sytuacja możliwa jest np. na małych parkignach przy

urzędach miejskich, gdzie w godzinach pracy urzędu dostęp do parkingu mają tylko pojazdy znajdujące się na „białej liście" np. pracownicy, aby po godzinach pracy urzędu dostęp do parkingu miały wszystkie pojazdy – szlaban otworzy się dla każdego jednak w systemie może pozostać informacja o numerach pojazdu parkującego, czasie jego pobytu na parkingu itp.).

Takie bogactwo funkcji pozwala na różnorodność zastosowań a wszelkiego rodzaju dane statystyczne wynikające z systemu pozwalają właścicielom parkingu na bardziej efektywne zarządzanie.

Systemy odczytu tablic rejestracyjnych mogą stanowić także fragment znacznie bardziej rozbudowanych systemów parkingowych.

W skład rozbudowanych systemów parkingowych oprócz systemu czytania rejestracji wchodzi także system zliczania wolnych miejsc parkingowych, który pozwala kontrolować ilość pojazdów na parkingu lub w danej strefie i automatycznie regulować ruchem wg zadanych parametrów. Czytelne tablice informacyjne wykonane w technologii LED informują o wolnych miejscach lub stanie parkingu „WOLNY/ ZAJĘTY". Zadaniem systemu jest usprawnienie organizacji ruchu na terenie parkingu poprzez naprowadzanie kierowców na wolne miejsca parkingowe. Kamery zewnętrzne i wewnętrzne wykrywają obecność pojazdów i automatycznie oznaczają wolne miejsce wykorzystując do tego kolorowe światła. Dane zbierane przez kamery ANPR na wjeździe, wyjeździe oraz wewnątrz parkingu są następnie zgromadzone w oprogramowaniu, dzięki czemu pozwalają określić liczbę wolnych miejsc parkingowych. Na dużych i bardziej skomplikowanych parkingach system dzięki zgromadzonym danym potrafi wskazać kierowcy kierunek ruchu oraz liczbę dostępnych miejsc w danej strefie parkingu – co zdecydowanie ułatwia kierowcom poruszanie się po parkingu w celu znalezienia wolnego miejsca. System ANPR pozwala także, w każdej chwili, na zlokalizowanie naszego pojazdu poprzez wprowadzenie w aplikację numeru rejestracyjnego – na tej podstawie dowiemy się, w którym sektorze parkingu jest nasze auto oraz jak tam dotrzeć. Ta funkcja potocznie nazywana jest lokalizatorem pojazdów.

Obraz z kamer pomocniczych znajdujących się wewnątrz parkingu może być wykorzystany również do odtworzenia zdarzeń parkingowych. Jeżeli dojdzie do incydentu, operator będzie w stanie prześledzić wydarzenia, sprawdzając alerty z konkretnych godzin.

System rozpoznawania tablic rejestracyjnych można także wykorzystać do ważenia pojazdów. Na podstawie rozpoznanego numeru rejestracyjnego, system odnajduje pierwsze ważenie i kojarzy je z drugim. Na podstawie różnicy dwóch mas zostaje określona masa netto towaru. Logika działania systemu może zostać każdorazowo dostosowana do konkretnych wymagań klienta.

Systemy LPR mogą być także wykorzystywane przez policję. Takie zastosowanie zostało zaimplementowane w Warszawie, gdzie policja wykorzystuje system do lokalizowania np. skradzionych pojazdów, czy też przy uruchomieniu procedury Child Alert – kiedy to sprawdzane jest czy samochód porywacza nie porusza się po terenie Warszawy. Wdrażanie systemu LPR w stolicy rozpoczęło się już 2021 r. a wartość projektu została oszacowana na kwotę 3766000zł z czego 85% sfinansował Norweski Mechanizm Finansowy 2014–2021. Pozostałą część 15% sfinansowała Komenda Stołeczna Policji.

Reasumując, opisane powyżej systemy LPR oraz sygnalizacji i zliczania wolnych miejsc parkingowych to dopiero namiastka tego jakie jeszcze systemy mogą być zainstalowane na współczesnym i nowoczesnym parkingu. Nie możemy bowiem zapominać o bileterkach, czyli terminalu wjazdowym oraz terminalu wyjazdowym, szlabanach, automatycznych kasach parkingowych czy też systemach sterowania oświetleniem w zależności od natężenia ruchu na parkingu. Urządzenia systemu parkingowego wykonują analizę zajętości parkingu, kontrolują ilość biletów w terminalach wjazdowych lub zarejestrowanych w systemie LPR, informują operatora o konieczności odebrania gotówki z automatycznych kas parkingowych. W przeciwieństwie do ręcznego poboru opłat za parkowanie, automatyczny system parkingowy pracuje autonomicznie i nie wymaga zaangażowania czynnika ludzkiego w pełnym wymiarze godzin pracy.

Robert Gabrysiak

WYKORZYSTANIE POSIADANEGO SPRZĘTU PRZEZ FUNKCJONARIUSZY SŁUŻBY WIĘZIENNEJ JAKO ISTOTNY ELEMENT PODNOSZĄCY BEZPIECZEŃSTWO JEDNOSTEK ORGANIZACYJNYCH SŁUŻBY WIĘZIENNEJ

Paweł Łuszcz

Zakłady Karne i Areszty Śledcze określane jako „jednostki organizacyjne”[1] to bardzo wyjątkowe i specyficzne miejsca. Wynika to nie tylko z faktu utrudnionego wejścia na ich teren (nie każdy kto ma chęć może wejść na ich teren) gdyż „pozbawienie lub ograniczenie wolności może nastąpić tylko na zasadach i w trybie określonych w ustawie”[2] ale także widocznej architektury (wysokie mury[3]). Wejście na jej teren jest ściśle określone w obowiązujących przepisach mianowicie np. „Rzecznik Praw Obywatelskich lub osoba przez niego upoważniona ma prawo wstępu w każdym czasie, bez ograniczeń, do zakładów karnych, aresztów śledczych innych miejsc, w których przebywają osoby pozbawione wolności oraz poruszania się po ich terenie”[4], a uprawnieniem Dyrektora tejże jednostki pozostało określenie czasu wejścia osób w związku z realizacją widzeń dla osadzonych „osoba uprawniona do widzenia z osadzonym wchodzi do jednostki organizacyjnej w ustalonych dniach i godzinach odbywania widzeń”[5]. Oprócz zasad wstępu Ustawodawca określił też prawa funkcjonariuszy w tym zakresie mianowicie – funkcjonariusze pełniący służbę w rejonie bramy głównej mają prawo do „legitymowania osób ubiegających się o wstęp oraz opuszczających teren jednostki organizacyjnej Służby Więziennej”[6]. Dostrzeżemy zatem, iż wyjątkowość jednostek organizacyjnych to nie tylko struktura wizualna – budowlana, ale także cytowane wyżej ustawowe uprawnienia pracujących funkcjonariuszy.

Zakres zadań funkcjonariuszy SW jest naprawdę duży i obejmuje on nie tylko te związane z szeroko pojętą resocjalizacją – prowadzenie oddziaływań penitencjarnych i resocjalizacyjnych wobec osób skazanych na karę pozbawienia wolności[7] ale również zabezpieczenie prawidłowego toku postępowania karnego[8], zapewnienie w zakładach karnych i aresztach śledczych porządku i bezpieczeństwa[9] oraz przeciwdziałanie narkomanii[10].

Co warte wskazania funkcjonariusze realizują swoje zadania nie tylko wobec osób osadzo-

[1] art. 8 pkt 1 ppkt 3 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz.U. 2022 r.poz. 655).

[2] art. 41 pkt 1 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U.1997 nr 78 poz. 483).

[3] „[…] wysokość ogrodzenia, wraz ze zwieńczeniem, winna wynosić 5–6 m, od poziomu terenu”. Wytyczne nr 2 Dyrektora Generalnego Służby Więziennej z dnia 4 czerwca 2013 r. w sprawie wymagań dla zabezpieczeń techniczno-ochronnych w jednostkach organizacyjnych służby więziennej, §2 pkt 2 ppkt2 lit. b.

[4] art. 8b §1 Ustawa Kodeks Karny Wykonawczy z dnia 6 czerwca 1997 r. (Dz. U. 2022 r. poz. 22, 655).

[5] §111 Rozporządzenia Ministra Sprawiedliwości z dnia 17 października 2016 r. (poz. 1804).

[6] art. 18 pkt 1 ppkt 2 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz. U. 2022 r.poz. 655).

[7] art. 2 pkt 2 ust 1 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz. U. 2022 r.poz. 655).

[8] art. 2 pkt 2 ust 2 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz. U. 2022 r.poz. 655).

[9] art. 2 pkt 2 ust 6 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz. U. 2022 r. poz. 655).

[10] Art. 5 pkt 2 ust 6 Ustawy o przeciwdziałania narkomanii z dnia 29 lipca 2005 r. (Dz. U. 2022 r. poz. 763,764).

nych w jednostkach ale także względem innych niż pozbawione wolności (także ich bagaży) wchodzących na jej teren np. w związku z realizacją widzeń dla osadzonych jak również pojazdów wjeżdżających i wyjeżdżających z terenu jednostki. Patrząc zatem całościowo na Zakłady Karne i Areszty Śledcze możemy powiedzieć, iż działania funkcjonariuszy i pracowników obejmują taki stan ich bytności aby na ich terenie nie doszło do zdarzenia nadzwyczajnego[11], czyli takiej sytuacji, która godziłaby w porządek i bezpieczeństwo.

Aby przeciwdziałać powstaniu sytuacji niebezpiecznych jak również wypełniać nałożone na Służbę Więzienną ustawowe obowiązki i zadania należy oprócz obowiązków i praw jakie posiadają funkcjonariusze sprawić, żeby dysponowali oni właściwym zapleczem technicznym tj. urządzeniami poprawiającymi nie tylko jakość ich pracy ale w głównej mierze jej efektywność.

Aby lepiej zobrazować i przedstawić posiadany i wykorzystywany sprzęt (urządzenia) przez funkcjonariuszy należy podzielić go na wskazane poniżej grupy[12]:

- po pierwsze to miejsca ich pełnienia służby;
- po drugie sprzęt przypisany do stanowiska;
- po trzecie to osobiste wyposażenie funkcjonariusza;
- po czwarte to te elementy obejmujące swym zakresem całą jednostkę organizacyjną.

Miejsce pełnienia służby:

Brama główna/biuro przepustek

Wejście do jednostki penitencjarnej jest miejscem istotnym z punktu widzenia bezpieczeństwa. To tutaj odbywa się cały ruch osobowy i towarowy. Dlatego funkcjonariuszy pełniących służbę w rejonie wejścia do jednostki (stanowisko bramowego, dyżurnego biura przepustek) trzeba wyposażyć w:

- urządzenia służące do identyfikacji legalności dokumentów tożsamości[13];

Nie bez znaczenia pozostaje przeszkolenie tychże funkcjonariuszy z zakresu sprawdzenia i poprawnej diagnozy czy dokument tożsamości jest autentyczny.

- urządzenia umożliwiające wykrycie osoby w pojazdach[14];
- bramowe i ręczne wykrywacze metalu i ceramiki[15];
- ręczne detektory – wykrywacze narkotyków[16];
- lustra inspekcyjne, obejmujące swym zakresem zarówno dach auta, jak i jego podwozie;
- urządzenie do bezpiecznego rozładowania i załadowania;
- bezobsługowy depozytor broni[17];
- skaner rentgenowski (RTG)[18].

Oddział mieszkalny

- urządzenie typu „ambu”[19];
- automated external defibrillator (AED)[20];

[11] Pkt 11 załącznika z dnia 3 stycznia 2018 r. nr 1 do zarządzenia nr 1/2018 Dyrektora Generalnego Służby Więziennej w sprawie służby dyżurnej w jednostkach organizacyjnych Służby Więziennej, zdarzeń mogących wystąpić w Służbie Więziennej oraz sposobu ich wyjaśniania i dokumentowania.

[12] Autor jest świadomy złożoności przedstawionej tematyki i problematyki, dlatego nie rości sobie praw do posiadania jedynej racji, a wypracowany model wyposażenia i sprzętu w trakcie realizacji zadań służbowych przedstawia jako propozycję do rozważań. Szerzej P. Łuszcz, Koncepcja Bezpieczeństwa Jednostki Penitencjarnej, Warszawa 2021 r.

[13] Sprzęt ten pozwoli na dokonanie technicznej analizy autentyczności dokumentu osób wchodzących do jednostki, jak również przyjmowanych do odbycia kary również TA. Wskazane urządzenie powinno również być wykorzystywane przez funkcjonariuszy i pracowników ewidencji zajmującymi się przyjęciami osadzonych do jednostki.

[14] To urządzenia potocznie nazywane – wykrywanie życia w pojazdach. Ich działanie polega na wychwyceniu i analizie czy w kontrolowanym pojeździe jest wyczuwalne bicie serca, tętno, puls.

[15] W obecnym czasie posiadany sprzęt wykrywa tylko elementy metalowe. Analizując zagrożenia, które wystąpiły na terenie krajów europejskich zasadnym jest, aby te urządzenia również posiadały funkcje wykrycia elementów ceramicznych, np. noży wykonanych z tego materiału.

[16] W potocznym języku funkcjonariuszy nazywane – elektronicznymi nosami. Urządzenie to działa na zasadzie swobodnego zasysania powietrza z badanego elementu i dokonania jego analizy pod kątem zawierania materiału narkotycznego. Przeprowadzone badanie osób powinno obejmować w pierwszej kolejności okolice dłoni, paska do spodni, stóp/obuwia.

[17] Urządzenie to wpłynie na poprawę pracy i bezpieczeństwo funkcjonariusza pełniącego służbę w rejonie bramy głównej. Osoba wchodząca na teren jednostki zobowiązana do zdeponowania broni wszystkie czynności z tym związane wykonuje sama (dlatego tak ważnym jest umieszczenie w tym rejonie urządzenia do bezpiecznego rozładowywania broni,), bez konieczności angażowania funkcjonariusza.

[18] Stacjonarne urządzenie, ważnym pozostaje aby przekazywany obraz posiadał funkcje maskowania stref intymnych.

[19] Jest to urządzenie stosowane do prowadzenia wentylacji oddechowej u pacjentów wymagających zastąpienia lub wspomagania tej funkcji. Umiejscowione w każdej dyżurce oddziałowego.

[20] Jedno urządzenie w każdym pawilonie mieszkalnym dla osadzonych.

- gaśnica wodno – mgłowa[21]
- kamera inspekcyjna, która ułatwi dokonywanie kontroli cel i pomieszczeń – również w innych miejscach nie tylko oddział mieszkalny ale także np. kuchnia, magazyn mundurowy, warsztat remontowy;
- ręczne wykrywacze metalu i ceramiki [22];
- ręczne detektory – wykrywacze narkotyków[23];
- lustra inspekcyjne;
- skaner rentgenowski (RTG)[24].

Wartownia

- minimum 100 sztuk kajdanek jednorazowych, które można wykorzystać w trakcie transportu czy też ewakuacji osadzonych z terenu jednostki organizacyjnej[25];
- automated external defibrillator (AED);
- urządzenia do bezpiecznego rozładowania i załadowania broni;
- myjka do ultradźwiękowego czyszczenia uzbrojenia.

Wyposażenie osobiste funkcjonariusza:

Co do zasady wskazanym jest aby wszyscy funkcjonariusze działu ochrony[26] byli wyposażeni w środki przymusu bezpośredniego i jest to obligatoryjne (bez względu na zajmowane stanowisko):

- ZK typu zamkniętego/areszt śledczy – kajdanki, pałka służbowa, ręczny miotacz substancji obezwładniających (RMP), nóż bezpieczny, rękawice nożoodporne, rękawiczki jednorazowe, opatrunek hydrożelowy, zarękawki[27], sygnalizator alarmowy.
- ZK typu półotwartego – kajdanki, ręczny miotacz substancji obezwładniających (RMP), nóż bezpieczny, rękawice nożoodporne, rękawiczki jednorazowe, opatrunek hydrożelowy, zarękawki, sygnalizator alarmowy;
- ZK typu otwartego – kajdanki, nóż bezpieczny, rękawice nożoodporne, rękawiczki jednorazowe, opatrunek hydrożelowy, zarękawki, sygnalizator alarmowy;
- kamery nasobne[28].

Elementy obejmujące swym zakresem całą jednostkę organizacyjną:

- urządzenia służące do zagłuszania sygnału telefonii komórkowej lub system wykrywania sygnału telefonii komórkowej;
- system antydronowy;
- psy służbowe specjalne;[29]
- psy służbowe patrolowo – obronne[30].

Wyposażenie funkcjonariuszy należy uzupełnić także o **tłumacze języka migowego** oraz w **tłumacze języków obcych**. Ich posiadanie i użytkowanie znacząco poprawi skuteczność działań związanych z bezpieczeństwem – stosowanie środków przymusu bezpośredniego oraz w codziennej komunikacji z osadzonym obcokrajowcem oraz osobą głuchoniemą. Posiadanie wskazanych urządzeń znacząco wpłynie na poprawę warunków pracy funkcjonariuszy, przestrzeganie praw człowieka oraz zniwelowanie sytuacji, które mogą nosić znamiona zdarzenia nadzwyczajnego.

Przedstawione wyposażenie, sprzęt który mógłby być wykorzystywany w trakcie realizacji zadań służbowych w jednostkach organizacyjnych SW nie tylko przyczyni się do poprawy warunków służby samych funkcjonariuszy, ale również wpłynie na zwiększenie bezpieczeństwa jednostek penitencjarnych. ■

mjr dr Paweł Łuszcz
specjalista ds. ochrony w OISW w Krakowie

[21] Oprócz posiadanego sprzętu ppoż. Obecnie zasadnym jest aby w oddziałach mieszkalnych znajdowała się co najmniej jedna gaśnica– służąca do gaszenia odzieży na człowieku.

[22] W obecnym czasie posiadany sprzęt wykrywa tylko elementy metalowe. Analizując zagrożenia, które wystąpiły na terenie krajów europejskich zasadnym jest, aby te urządzenia również posiadały funkcje wykrycia elementów ceramicznych, np. noży wykonanych z tego materiału.

[23] W potocznym języku funkcjonariuszy nazywane – elektronicznymi nosami. Urządzenie to działa na zasadzie swobodnego zasysania powietrza z badanego elementu i dokonania jego analizy pod kątem zawierania materiału narkotycznego. Przeprowadzone badanie osób powinno obejmować w pierwszej kolejności okolice dłoni, paska do spodni, stóp/obuwia.

[24] To ręczne urządzenie mogące być wykorystywane zarówno względem osób oraz bagaży i posiadanych rzeczy.

[25] Ich liczba może być zwiększona w zależności od pojemności normatywnej jednostki organizacyjnej.

[26] Funkcjonariusze innych działów są wyposażani w sprzęt w sytuacji bezpośredniego kontaktu z osadzonymi, np. dział kwatermistrzowski – szef kuchni. Kobiety, które pełnią służbę/pracę w innych komórkach niż dział ochrony w trakcie bezpośredniego kontaktu z osadzonymi posiadają na wyposażeniu indywidualny sygnalizator alarmowy.

[27] Jest to element odzieży wykorzystywany w okresie letnim, kiedy funkcjonariusze pełnią służbę w umundurowaniu z którym rękawem – ten element pozwala zabezpieczyć przedramiona w sytuacji zagrożenia, stosowania śpb.

[28] Ten rodzaj wyposażenia posiada tylko dowódca zmiany i jego zastępca. Urządzenie uruchamiane tylko w sytuacji zagrożenia.

[29] §10 pkt 1 Zarządzenia nr 89/20221 Dyrektora Generalnego Służby Więziennej z dnia 29 grudnia 2021 r. w sprawie określenia kryteriów zdrowotnych i użytkowych doboru, w tym cech przydatności, psów w Służbie Więziennej oraz sposobów ich użytkowania. Psy wyszkolone na specjalistycznych kursach do odnajdywania substancji narkotycznych.

[30] §10 pkt 2 Zarządzenia nr 89/20221 Dyrektora Generalnego Służby Więziennej z dnia 29 grudnia 2021 r. w sprawie określenia kryteriów zdrowotnych i użytkowych doboru, w tym cech przydatności, psów w Służbie Więziennej oraz sposobów ich użytkowania, art. 19 pkt 4 Ustawy o Służbie Więziennej z dnia 9 kwietnia 2010 r. (Dz. U. 2022 r. poz. 655). Psy te mogą również pełnić służbę w specjalnych sektorach zabezpieczając jednostkę organizacyjną przed ucieczką osadzonego.

ZASILANIE AWARYJNE ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZEŃ

Elektroniczne systemy zabezpieczeń, ze względu na rolę jaką pełnią, powinny móc pracować stale, także w przypadku wystąpienia przerwy w dostawie energii elektrycznej. W związku z tym do zasilania urządzeń wchodzących w skład tego typu instalacji, wykorzystuje się zasilacze buforowe – źródła mogące zapewnić ciągłość zasilania nawet przez wiele godzin.

Wśród szerokiej gamy zasilaczy buforowych dostępnych na rynku, największą efektywność oferują konstrukcje z bezpośrednim przetwarzaniem napięcia sieciowego. Urządzenia wyposażone w przetwornicę impulsową, obniżają napięcie sieciowe i dostosowują do wymagań danej instalacji. Wykorzystują akumulatory zewnętrzne, jako awaryjne źródło prądu stałego. W momencie awarii sieci lub odłączenia od niej, zgromadzona w nich energia kierowana jest na wyjście zasilające. Z kolei podczas normalnej pracy całego systemu, podłączone akumulatory są ładowane i utrzymywane w stanie gotowości. Doskonałym przykładem impulsowych zasilaczy buforowych są dwa uniwersalne modele produkowane przez firmę SATEL: APS-1412 oraz APS-724.

Dwa urządzenia – wiele możliwości

Podstawowe parametry tych urządzeń, czyli maksymalny prąd wyjściowy oraz znamionowe napięcie wyjściowe, „zakodowane” są w ich nazwach. I tak wydajność prądowa modelu APS-1412

instalacja alarmowa

instalacja CCTV

kontrola dostępu

instalacja domofonowa

automatyka budynkowa

to aż 14 A lub 12 A (zasilanie urządzeń) + 2 A (ładowanie akumulatorów), zaś napięcie wyjściowe to 12 V DC. W przypadku APS-724 wynoszą one odpowiednio 7 A (lub 6 A i 1 A) i 24 V DC.

Dostępność dwóch modeli o różnych napięciach znamionowych daje odbiorcy możliwość wyboru jednostki, która będzie odpowiadała parametrami docelowej instalacji: alarmowej, monitoringu wizyjnego, domofonowej, kontroli dostępu, automatyki budynkowej czy przemysłowej i wielu innych.

Wysoki prąd wyjściowy umożliwia włączenie do systemu pojedynczych dużych obciążeń lub wielu mniejszych. Dla przykładu, instalacja CCTV, wykorzystująca tylko jeden APS-1412, może obejmować nawet 50 kamer zasilanych prądem nieprzekraczającym 250 mA. Ten konkretny model oferuje także możliwość integracji z niektórymi urządzeniami z portfolio SATEL, m.in. ekspanderami wejść INT-E lub wyjść INT-ORS, centralami kontroli dostępu ACCO-NT czy kontrolerami przejść ACCO-KP, jak również uniwersalnymi modułami: komunikacyjnym GSM-X LTE i monitorującymi GPRS-A LTE lub ETHM-A. Wykorzystuje się w tym celu specjalny kabel wpinany do 3-pinowych złącz APS. Dzięki temu można nie tylko szybko połączyć zasilacz z odbiornikiem – będzie on wówczas odbierał informacje o stanie zasilania AC, stanie podłączonego akumulatora oraz o ewentualnym przeciążeniu zasilacza.

Dla lokalnej sygnalizacji stanu APS-1412 oraz APS-724 wyposażone są w cztery różniące się kolorami diody LED. Za ich pomocą urządzenie sygnalizować może status wyjścia zasilania, akumulatora, zasilania AC, a także przekroczenie temperatury zasilacza. Oprócz tego wykryte awarie sygnalizowane są akustycznie oraz na czterech wyjściach typu OC. Na wyjścia te wystawiona może być informacja o: braku zasilania

AC, braku akumulatora, rozładowanym akumulatorze lub jego zbyt duża rezystancja wewnętrzna, przeciążenie zasilacza oraz przekroczeniu dopuszczalnej temperatury pracy. Stany wyjść wykorzystać można np. w ramach systemów automatyki przemysłowej.

Stabilne parametry pracy

Warto podkreślić, że opisywane urządzenia zasilające charakteryzują się wysoką sprawnością energetyczną przekraczającą 90%. Konkretnie mowa o max. 91% w przypadku zasilacza APS-1412 i aż 94% w APS-724. Dzięki optymalizacji konstrukcji polegającej między innymi na wykorzystaniu wysokosprawnych podzespołów, nie jest wymagane zakładanie dodatkowego chłodzenia – emisja ciepła jest niezwykle niska. Ewentualne jego nadwyżki są skutecznie odprowadzane przez obudowę wykonaną z anodowanego aluminium. Oczywiście, ze względów bezpieczeństwa, zasilacze nie powinny być instalowane w szczelnej zabudowie – przepływ powietrza dookoła powinien być swobodny.

Wspomniana wyżej wysoka sprawność energetyczna oraz duża wydajność prądowa to nie jedyne zalety zasilaczy. Idą one bowiem w parze z bardzo dobrymi, stabilnymi parametrami pracy, nawet przy dużych wahaniach napięcia sieciowego. Wynika to z zastosowania układów scalonych, których właściwością jest dynamiczne dostosowywanie się do zmiennych warunków. Zastosowano także aktywny układ korekcji współczynnika mocy PFC (nawet do 0,99). Precyzyjna regulacja napięcia, kontrola stanu naładowania akumulatora (z pomiarem rezystancji wewnętrznej), a także funkcja automatycznego odłączenia w przypadku nadmiernego rozładowania – przedłużają żywotność awaryjnego źródła zasilania, bez ryzyka jego uszkodzenia. Wysoki poziom bezpieczeństwa zapewnia zabezpieczenia: przeciwprzeciążeniowe (OCP), przeciwprzepięciowe (OVP) oraz przeciwzwarciowe (SCP).

Zgodność z normami

Oba opisywane zasilacze w zakresie bezpieczeństwa odpowiadają wymogom normy EN 60950-1, natomiast biorąc pod uwagę kryterium kompatybilności elektromagnetycznej, a konkretnie poziomu przewodzonych i promieniowanych zakłóceń EMI, są zgodne z normą EN 55011 Class B. Z kolei spełnianie przez APS 1412 wymogów dla Stopnia zabezpieczenia Grade 2 według normy EN 50131 jest niezwykle ważne w sytuacji, gdy to źródło energii ma pracować w ramach systemu sygnalizacji włamania i napadu.

Gdyby jednak wymagany był wyższy stopień zabezpieczenia (Grade 3), warto dodać, że w ofercie SATEL dostępny jest inny model zasilacza, który spełnia tak rygorystyczne wymagania.

Mowa tu o APS-612 – urządzeniu charakteryzującemu się znamionowym napięciem wyjściowym 12 V DC i wydajnością prądową 3 A. ■

Satel
MADE TO PROTECT

Artykuł Firmy **SATEL**

Kontrola dostępu w biurowcach i budynkach użyteczności publicznej jest w tej chwili powszechnym standardem, a często koniecznym wymogiem narzuconym przez inwestora. Kiedy powstaje nowy obiekt, rozbudowana koncepcja takiego systemu pojawia się już na etapie projektowania, a prace przygotowawcze do instalacji trwają na każdym etapie budowy. Ponieważ większość dostępnych na rynku rozwiązań bazuje na instalacjach niskoprądowych, do ich montażu niezbędne jest rozprowadzenie po budynku odpowiedniego okablowania oraz zaplanowanie zabezpieczeń napięcia, w postaci UPS-ów czy agregatów.

Znacznie większe wyzwanie stanowi wprowadzenie systemu kontroli dostępu do istniejącego i funkcjonującego budynku, w którym na co dzień działają firmy i przebywają pracownicy. Taka operacja kojarzy się nieodłącznie z niedogodnościami w postaci prac remontowych, związanych z kuciem ścian, kładzeniem okablowania, wymianą stolarki drzwiowej oraz instalacją wielu skomplikowanych i drogich urządzeń.

Jeszcze bardziej złożonym zagadnieniem jest montaż kontroli dostępu w budynkach zabytkowych, objętych ochroną konserwatora zabytków. Często mieszczą się w nich hotele, muzea, szpitale, jednym słowem instytucje, w których na co dzień funkcjonują zarówno pracownicy jak i osoby z zewnątrz, a które trzeba w sposób szczególny chronić przed nieuprawnionym dostępem.

Firma Winkhaus Polska posiada w swojej ofercie rozwiązanie, pozwalające zabezpieczyć obiekty i poszczególne pomieszczenia w budynku przed nieautoryzowanym dostępem, a którego instalacja przebiega bez prowadzenia prac remontowych, ingerencji w strukturę budynku, czy nawet wymiany drzwi i zamków.

Mowa tu o elektronicznym systemie blueSmart, przeznaczonym do wszelkiego rodzaju obiektów, przede wszystkim biurowców i przedsiębiorstw, ale też szkół, szpitali, obiektów użyteczności publicznej, budynków zarówno nowoczesnych jak i historycznych.

Instalacja bez przygotowań

System blueSmart można zamontować na każdym etapie eksploatacji obiektu. Instalacja nie wymaga żadnych wcześniejszych zabiegów, nie ma znaczenia stan budynku ani jego przeznaczenie, liczba użytkowników i stopień skomplikowania praw dostępu.

Brak okablowania

Dzięki wykorzystaniu sieci wirtualnej system blueSmart nie wymaga okablowania i może być instalowany także w obiektach już wykończonych i użytkowanych. Rozwiązuje także wszelkie problemy z instalacją zabezpieczeń w drzwiach całoszklanych.

Łatwy montaż

Wkładki elektroniczne wymiarami i kształtem nie różnią się od standardowych wkładek bębenkowych. Dzięki temu ich montaż w drzwiach jest bardzo prosty – polega na wymianie wkładki mechanicznej na jej odpowiednik elektroniczny.

Wysoki poziom bezpieczeństwa

System blueSmart łączy zalety bezpieczeństwa systemów mechanicznych z elastycznością zaawansowanej elektroniki

– drzwi są w pełni zaryglowane, jak w tradycyjnym zamku, a nie tylko zablokowane przez elektrozaczep.

System posiada zintegrowane moduły czasowe, rejestruje każdą operację lub zamiar operacji dokonany przez autoryzowany lub nieautoryzowany klucz, wraz z informacją o czasie i godzinie jej wykonania. Klucz zagubiony lub skradziony zostaje wyeliminowany przez administratora z systemu i staje się całkowicie bezużyteczny dla nieuprawnionego posiadacza.

Elastyczne, bezkosztowe zmiany uprawnień odpowiednio do zmian w organizacji

Elastyczność blueSmarta daje możliwość praktycznie nieograniczonego dopasowania systemu do zmieniającej się organizacji obiektów. Uprawnienia są zmieniane przez administratora systemu za pomocą kilku kliknięć.

System pozwala na rozszerzenie o nowe wkładki i klucze w dowolnym momencie. Może składać się nawet ze 195 tysięcy komponentów. Jego mniejszy „brat", system blueCompact, przeznaczony do małych firm, zbudowany z maksymalnie 25 wkładek i 99 kluczy, obsługiwany jest za pomocą aplikacji na smartfonie. Ten sam system może funkcjonować w więcej niż jednym budynku i różnych, nawet oddalonych od siebie lokalizacjach.

Cenioną przez firmy zaletą systemu jest możliwość zainstalowania go tylko w wybranych drzwiach, zamykających pomieszczenia strategiczne z punktu widzenia firmy. To na przykład serwerownia lub pomieszczenie, w którym przechowywane są dane osobowe czy inne wrażliwe informacje.

Przy zastosowaniu wkładek elektronicznych korzystamy z nieograniczonej liczby kombinacji dostępu i użytkowników, a w razie zagubienia lub kradzieży klucza nie ma potrzeby wymiany zamknięć w obiekcie, jedynym kosztem jest zakup nowego klucza.

Dyskretna stylistyka

Wkładki nie posiadają wystających elementów, są zlicowane ze skrzydłem drzwi i dopasowują się do drzwi w różnych stylach, zarówno nowoczesnych, jak i zabytkowych.

Kompatybilność

System blueSmart jest kompatybilny z innymi systemami dostępu zarządzanymi online. Wówczas pod kontrolą można mieć nie tylko otwieranie drzwi, ale także system rejestracji czasu pracy, można sterować windą albo uruchomić maszynę produkcyjną lub biurową drukarkę. Przy użyciu klucza użytkownik może otwierać szlabany, sterować oświetleniem czy uzbroić system alarmowy. Klucze mogą być dodatkowo wyposażone w transpondery pomagające skoordynować obsługiwane systemy.

Elementy systemu

blueSmart składa się z wyposażonych we własne zasilanie wkładek elektronicznych, kluczy oraz czytników aktualizujących, które pełnią rolę interfejsów między komponentami systemu a oprogramowaniem sterującym. Zespół komponentów dopełnia wprowadzona niedawno klamka elektroniczna. Wszystkie te elementy komunikują się między sobą bezprzewodowo, bez zasilania zewnętrznego i w sposób zaszyfrowany, z zachowaniem najwyższych standardów bezpieczeństwa.

Wkładki elektroniczne

Wkładki zasilane są wewnętrznymi bateriami litowymi, a ich stan kontrolowany jest na bieżąco przez oprogramowanie, które sygnalizuje z odpowiednim wyprzedzeniem konieczność wymiany. Trwałość baterii gwarantowana jest nawet do 10 lat w przypadku wkładek zewnętrznych i do 5 lat w przypadku wkładek wewnętrznych, w zależności od częstotliwości użycia. W znormalizowanych warunkach atmosferycznych baterie zatem mogą „obsłużyć" nawet do 25 tysięcy cykli.

Klucze elektroniczne

Istotnym elementem systemu jest klucz, będący nośnikiem informacji między pozostałymi komponentami. Na podstawie zapisanych w kluczu danych wkładka pozwala, bądź nie, na obrót klucza i tym samym odryglowanie lub zaryglowanie zamka. Transmisja danych między kluczem a wkładką oparta jest na technologii RFID.

Każdy klucz przypisany jest do konkretnego użytkownika i może działać tylko w godzinach wyznaczonych przez administratora. Klucz po wyznaczonym czasie traci swoje uprawnienia. Przed kolejnym dniem pracy użytkownik aktualizuje klucz w czytniku i wtedy może otworzyć drzwi, do których ma przydzielony dostęp.

Sam klucz jest wykonany z solidnego tworzywa, estetyczny, dostępny w kilku kolorach. Nie zawiera części łatwych do uszkodzenia ani ostrych mogących przeciąć kieszeń czy torebkę. Jest odporny na wodę i działanie środków dezynfekujących, można go bez szkody nawet wyprać w pralce.

Klamka elektroniczna

Najnowszy komponent systemu, elektroniczna klamka do drzwi wewnętrznych ETB-IM, również działa bezprzewodowo i może być zainstalowana wszędzie tam, gdzie uzasadnienie ma montaż drzwi na kartę zbliżeniową lub kod. Jest idealnym rozwiązaniem do drzwi w hotelach i biurach.

Czytnik

Czytnik służy komunikacji pomiędzy oprogramowaniem blueSmart a elementami systemu. Może być umieszczony na zewnątrz lub wewnątrz budynku. Pracownicy przy wejściu do obiektu aktualizują w czytniku swoje klucze, pobierają przypisane im uprawnienia i przekazują do systemu informacje zapisane na ich własnych kluczach. Czytnik online jako jedyny element systemu wymaga okablowania, jednak w przypadku braku zasilania kontrola zostaje w pełni zachowana, bez konieczności instalacji urządzeń podtrzymujących napięcie. ■

Magdalena Madej
Specjalistka ds. systemów zabezpieczeń – Winkhaus Polska

ZASILACZE DO URZĄDZEŃ PRZECIWPOŻAROWYCH – WYMAGANIA CNBOP

Zabezpieczenie przeciwpożarowe to jedno z najważniejszych zabezpieczeń budynku mające bezpośredni wpływ na bezpieczeństwo jego użytkowników. Odpowiednio zaprojektowana instalacja zasilająca urządzenia przeciwpożarowe zapewnia ich właściwe funkcjonowanie zarówno w stanie gotowości, jak i w czasie pożaru.

Robert Gabrysiak

Wymagania dotyczące zasilaczy urządzeń przeciwpożarowych określono w odpowiednich normach i rozporządzeniach. Podstawową normą określającą parametry i funkcje zasilaczy do urządzeń przeciwpożarowych jest norma PN-EN 54-4, którą można nabyć w następujących wersjach:

- PN-EN 54-4:2001/A2:2007 – wersja polska.
  W niniejszym załączniku: – dodano wymagania na zasilacze stanowiące integralną część innych urządzeń sygnalizacji pożarowej – uaktualniono i dodano nowe wymagania dotyczące odporności EMC – dokonano szeregu różnych zmian w celu poprawienia błędów i lepszego odzwierciedlenia bieżącej praktyki;
- PN-EN 54-4:2001/A1:2004 – wersja polska.
  W tej zmianie do normy dotyczącej zasilaczy stosowanych w systemach sygnalizacji pożarowej określono powiązanie normy z dyrektywą 89/106/EEC Wyroby budowlane;
- PN-EN 54-4:2001 – wersja polska.
  W normie określono wymagania i badania urządzeń zasilających, będących częścią systemów sygnalizacji pożarowej. W szczególności podano zasady współpracy zasilaczy z rezerwowym źródłem zasilania (baterią akumulatorów) oraz wymagania w zakresie badań środowiskowych i kompatybilności elektromagnetycznej.

Kolejną normą stanowiąca o zasilaczach do urządzeń p.poż jest norma PN-EN 12101-10:2007 – wersja polska „Systemy kontroli rozprzestrzeniania dymu i ciepła – Część 10: Zasilacze", która w swoim zakresie określa wymagania i podaje metody badań dla podstawowego i dodatkowego elektrycznego i pneumatycznego wyposażenia zasilającego energią, przeznaczonego do sto-

sowania w systemach do kontroli rozprzestrzeniania dymu i ciepła w budynkach. Podaje także wymagania dotyczące oceny zgodności tego wyposażenia.

Poza normami nie mniej ważne są certyfikaty CNBOP-PIB (Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy). Jednostka Certyfikująca CNBOP-PIB prowadzi procesy dopuszczenia wyrobów służących zapewnieniu bezpieczeństwa publicznego, ochronie zdrowia, życia oraz mienia, wprowadzane do użytkowania w jednostkach ochrony przeciwpożarowej oraz wykorzystywane przez te jednostki do alarmowania o pożarze lub innym zagrożeniu oraz do prowadzenia działań ratowniczych, a także wyrobów stanowiących podręczny sprzęt gaśniczy.

Wykaz wyrobów podlegających procesowi dopuszczenia zawarto na stronie Instytutu pod linkiem: https://www.cnbop.pl/uslugi/jednostka-certyfikujaca/wykazy/wykaz-p-d.pdf.

Warto zwrócić uwagę, że w punkcie 81 wykazu zawarto zasilacze urządzeń przeciwpożarowych, które badane są wg standardu CNBOP-PIB 0007:2016 (wydanie 3) „Zasilacze do urządzeń przeciwpożarowych). Standard ten w swoim zakresie obejmuje „*aktualne informacje dotyczące stanu prawnego i normalizacyjnego oceny zgodności wyrobów budowlanych służących do ochrony przeciwpożarowej, takich jak zasilacze do urządzeń przeciwpożarowych mające istotne znaczenie zarówno dla projektantów, instalatorów i konserwatorów, jak również funkcjonariuszy pionów kontrolno-rozpoznawczych Państwowej Straży Pożarnej, organów nadzoru budowlanego oraz inwestorów czy deweloperów. Specjalista wzbogacony wiedzą zawartą w niniejszej publikacji będzie świadom tego, jakie wymagania powinien spełniać wyrób oraz jakie dokumenty i oznakowanie na wyrobie potwierdzają spełnienie określonych wymagań. Zdobyta w ten sposób wiedza umożliwi wybór wyrobu, który spełnia aktualne wymagania, jest bezpieczny oraz w pełni funkcjonalny. Standard identyfikuje wymagane dokumenty dla zasilaczy, jak również istotne wymagania czy funkcjonalności, jakie powinny posiadać certyfikowane i dopuszczone zasila-*

Reklama

Tabela 1.

Klasa środowiskowa	Środowisko	Zakres temperatur pracy (°C)	Minimalny stopień IP (zasilacze elektryczne)
1	Wewnętrzne, czyste, niska temperatura	od -5 do +40	30
2	Wewnętrzne, czyste, wysoka temperatura	od -5 do +75	42
3	Wewnętrzne – korozyjne, wilgotne lub zewnętrzne	od -5 do +75	54
4	Zewnętrzne – korozyjne	od -25 do +75	65

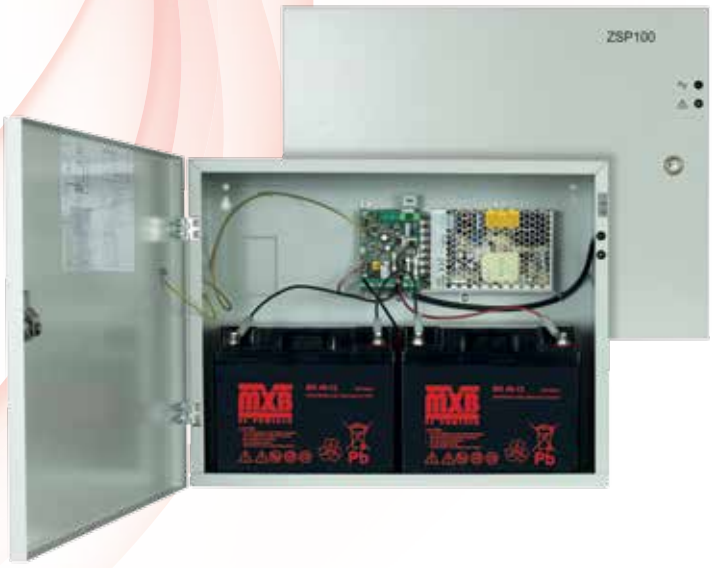
Źródło: 1-10:2005+AC:2007 Systemy kontroli rozprzestrzeniania dymu i ciepła – Część 10: Zasilacze.

cze". Oczywiście powyżej wspomniany standard „opiera się" na wspomnianych normach i dzieli zasilacze na:

- Zasilacze stosowane w systemach sygnalizacji pożarowej;
- Zasilacze stosowane w dźwiękowych systemach ostrzegawczych;
- Zasilacze stosowane w systemach kontroli rozprzestrzeniania dymu i ciepła;
- Zasilacze stosowane w systemach sterowania oddzieleniami przeciwpożarowymi.

Wszystkie z wyżej wymienionych zasilaczy mogą dostarczać energię z podstawowego źródła zasilania, którym jest sieć elektroenergetyczna a w przypadku jej zaniku – ze źródeł rezerwowych takich jak bateria akumulatorów.

Norma PN-EN 54-4 precyzuje szereg wymagań jakie powinny spełniać zasilacze znajdujące zastosowanie w systemach ochrony przeciwpożarowej. Pod względem stopnia ochrony IP norma określa, że zasilacze systemów przeciwpożarowych powinny posiadać obudowy o minimalnym stopniu IP na poziomie IP30. Nieco inaczej podział ten przedstawia się dla zasilaczy systemów kontroli rozprzestrzeniania dymu i ciepła, który zawarto w normie EN 12101-10:2005+AC:2007. Tutaj klasyfikacja zasilaczy przedstawia się jak w tabeli 1.



Kolejne wymogi wspomnianych powyżej norm dotyczą znakowania zasilaczy. W przypadku normy PN-EN 54-4 od cechowania zasilaczy wymaga się aby zawierały:

- numer normy europejskiej tj. EN 54-4;
- nazwę lub znak towarowy producenta lub dostawcy;
- numer typu lub innego oznaczenia zasilacza;
- kod lub numer identyfikujący okres produkcji zasilacza.

W przypadku zasilaczy posiadających swoją obudowę należy na etykiecie cechującej zawrzeć minimum pierwsze trzy informacje. Natomiast, gdy zasilacz wbudowany jest w obudowę urządzenia zasilanego tym zasilaczem to na cechowaniu należy zawrzeć przynajmniej informacje dotyczące numeru normy europejskiej oraz nazwy i znaku towarowego producenta czy dostawcy.

Nieco „bogatsze" znakowanie wymagane jest wg normy PN-EN 12101-10 wg której powinno ono zawierać informacje na temat:

- numeru normy europejskiej tj. EN 12101-10;
- nazwy lub znaku towarowego producenta lub dostawcy;
- numeru typu lub innego oznaczenia zasilacza;
- kodu lub numeru identyfikującego okres produkcji, partię lub jednoznaczny wzorzec zasilacza;
- klasy według normy europejskiej EN 12101-10;
- danych technicznych zawierających:
  - czas przerwy
  - maksymalną pojemność baterii akumulatorów
  - wartości wejściowe
  - wartości wyjściowe
- ostrzeżeń, jeśli są wymagane.

Minimalne wymagania cechowania dla zasilaczy we własnej obudowie powinny zawierać informacje o numerze normy europejskiej tj. EN 12101-10, nazwie lub znaku towarowym producenta lub dostawcy, numerze typu lub innego oznaczenia zasilacza oraz ostrzeżenia – jeśli są wymagane. W przypadku zasilaczy wbudowanych w obudowę urządzenia, które zasilają na zewnątrz obudowy powinno umieścić się informacje o numerze normy europejskiej tj. EN 12101-10, nazwie lub znaku towarowym producenta lub dostawcy oraz ostrzeżenia – jeśli są wymagane.

Ponadto wspomniane powyżej normy narzucają jeszcze szereg innych wymagań, z których kilka wymieniono poniżej:

a) dla zasilaczy w oddzielnej obudowie wymaga się aby posiadały one dwa niezależne wyjścia zabezpieczone przed zwarciem oddzielnymi bezpiecznikami. Jeśli ten wymóg nie jest spełniony to zasilacze nie mogą być wszędzie wykorzystane – np. nie mogą być użyte do zasilania central dźwiękowego systemu ostrzegawczego;
b) zasilacz podczas zasilania z rezerwowego źródła zasilania powinien mieć możliwość odcięcia wyjścia w momencie np. gdy napięcie baterii akumulatorów osiągnie pewien określony przez producenta poziom;
c) wymaga się odpowiedniej sygnalizacji przepalenia bezpiecznika baterii, uszkodzenia obwodu ładowania, niskiego napięcia wyjściowego, wysokiego napięcia wyjściowego czy też uszkodzenia zasilacza;
d) Kluczowe wymagania stawia się tez odnośnie zabezpieczeń przed przepięciem, zwarciem oraz przeciążeniem;
e) Każdy zasilacz powinien posiadać wyjście awarii zbiorczej (alarm), wyjście techniczne EPS oraz wyjście techniczne APS.

Oczywiście producenci zasilaczy oferują zdecydowanie większą ilość dostępnych rozwiązań technicznych – wybiegając zdecydowanie poza wymagania norm i rozporządzeń. Przykładowo umieszczają w swoich zasilaczach wejście sygnału awarii zewnętrznej, sterowane wyjście przekaźnikowe, czy funkcję zdalnego testu akumulatorów, pomiaru napięcia sieci zasilającej 230V oraz sygnalizację otwarcia obudowy.

Powyżej wymienione wymagania dotyczące zasilaczy to tylko nieliczne z tych, które zawarto w przytaczanych normach i standardzie CNBOP. Wszystkich zainteresowanych szczegółowymi informacjami odsyłam do tychże norm oraz na stronę Instytutu Badań i Certyfikacji CNBOP – skąd można dowiedzieć się także jak krok po kroku przebiega proces certyfikacji zasilaczy oraz innych urządzeń przeciwpożarowych. Bowiem należy pamiętać, że zasilacze do urządzeń przeciwpożarowych mogą być wprowadzone do obrotu a następnie do użytkowania w Polsce tylko i wyłącznie wtedy, gdy producent sporządził deklarację właściwości użytkowych oraz niezależnie uzyskał świadectwo dopuszczenia. ■

Źródła wiedzy:
1. www.cnbop.pl
2. www.pkn.pl

Robert Gabrysiak

Reklama

CYBER THREAT INTELLIGENCE

Grzegorz Data

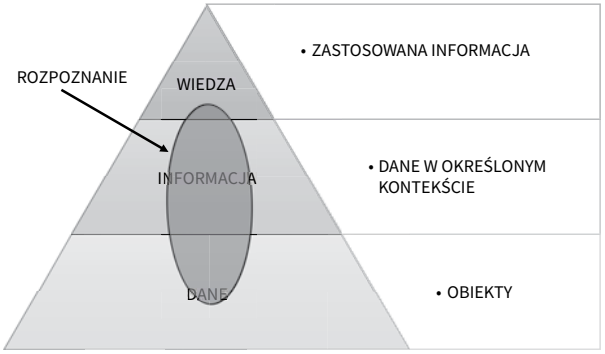
Cyber threat intelligence – ze względu na wielorakie znaczenia słowa *intelligence*, które można tłumaczyć jako rozpoznanie, wywiad, czy nawet analizę zagrożeń. Najbardziej chyba odzwierciedlające ideę pojęcia tłumaczenia to rozpoznanie zagrożeń cybernetycznych (informatycznych). Jedna z najkrótszych definicji (przez analogię do *business intelligence*) to proces przekształcania danych o zagrożeniach cybernetycznych w informację (dane w określonym kontekście) a informacji w wiedzę. Dane to np. fakty, adresy, ciągi znakowe, informacja w tym sensie są to dane w określonym kontekście czy też relacji, wiedza zaś to interpretacja lub wykorzystanie posiadanych informacji do rozwiania problemu lub podjęcia decyzji. Rozpoznanie było by wiec interpretacją opartą na dowodach, zebranych aby zidentyfikować cele, motywacje techniki taktyki lub procedury sprawców zagrożenia. Rozpoznanie pomaga zrozumieć, złagodzić lub wyeliminować zagrożenia. Definicję powyższą dobrze przedstawia schemat na rysunku 1 zaproponowany przez Bank of England (Bank of England, 2016c, p. 13).

Stosowanie tradycyjnych mechanizmów zabezpieczeń jest wystarczające na wewnętrzne potrzeby organizacji, ale w prawie nie zauważa ryzyk, które powodują zagrożenia pochodzące z zewnątrz. Hacktywizm, cyberkonflikty między państwami czy szpiegostwo przemysłowe to stałe elementy listy zagrożeń. Wskazane zatem jest, aby mechanizmy obrony przed nimi miały charakter wyprzedzający i powinny funkcjonować niczym sprawny wywiad, gdyż właściwe jest założenie, że skuteczny może zostać przeprowadzony z prawdopodobieństwem graniczącym z pewnością. O ile tradycyjne cyberbezpieczeństwo obejmuje rekrutację i zatrudnienie ekspertów zajmujących się bezpieczeństwem informatycznym, ustalenie formalnych regulacji i polityk bezpieczeństwa oraz rozmieszczenie urządzeń i aplikacji zabezpieczających infrastrukturę techniczną tak rozpoznanie zagrożeń cybernetycznych (Cyber Threat Intelligence) opiera się na gromadzeniu wiedzy o zagrożeniach stosując: biały wywiad (OSINT–Open Source INTelligence), informacje z mediów społecznościowych (SOCMINT – SOCial Media INTelligence) oraz informacje ze źródeł osobowych (HUMINT – HUMan INTelligence) a także wiedzę z deep– i dark–web. Kluczowym zadaniem cybernetycznego rozpoznania jest badanie, analiza trendów oraz zmian w takich obszarach jak cyberprzestępczość, cyberaktywizm (np. Anonymous) oraz cyberszpiegostwo (np. ataki APT). Oczywiście wiedza ta musi być wzbogacona informacjami z własnej infrastruktury, gromadząc i korelując dane o zda-

rzeniach bezpieczeństwa. Należy zmienić optykę – nie zastanawiać się czy organizacja jest bezpieczna, lecz jakie czynności zostaną podjęte, gdy zostaniemy zaatakowani. Konieczna jest proaktywna postawa z gotowością na cyberatak.

Według brytyjskiego Ośrodka Ochrony Infrastruktury Narodowej (CPNI), istnieją cztery rodzaje rozpoznania zagrożeń przedstawione na rysunku 2. (National Cyber Security Centre, 2015, p. 4), podobnie definiuje je brytyjska firma MWR Infosecurity współpracująca z CERT w Wielkiej Brytanii (MWR Infosecurity, 2015).

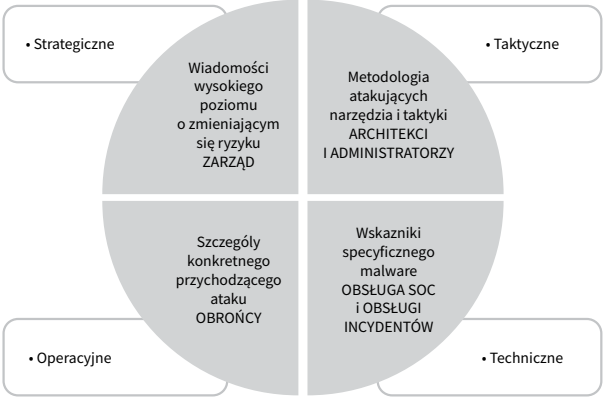
- **Techniczne**: Techniczne rozpoznanie cyberzagrożeń zawiera szczegółowe informacje o zasobach napastnika, takich jak narzędzia, kanały dowodzenia i kontroli oraz infrastruktura. Różni się od rozpoznania taktycznego tym, że koncentruje się na konkretnych wskaźnikach, szybkiej dystrybucji i reakcji, a zatem ma krótszy użyteczny okres eksploatacji. Fakt, że atakujący używa konkretnego złośliwego oprogramowania, to rozpoznanie taktyczne, a wskaźniki przeciwko konkretnemu skompilowanemu przykładowi to rozpoznanie techniczne. Typowe przykłady wywiadu dotyczącego zagrożeń technicznych obejmują sumy szkodliwego oprogramowania lub phishingowych przynęt-dokumentów MD5, nagłówki wiadomości e-mail typu phishing, adresy IP dla urządzeń końcowych C2 lub nazw domen używanych przez C2. Idealne wskaźniki powinny pochodzić z aktywnych kampanii, które są obecnie doświadczane przez inne organizacje. Dzięki szybkiemu włączeniu tych wskaźników do infrastruktury defensywnej, takich jak firewalle, urządzenia filtrujące poczta i rozwiązania zabezpieczające przed wyciekiem danych, organizacje mogą starać się wykrywać napastników – zarówno wtedy, gdy najpierw atakują, czy we wczesnych stadiach ataku. Przeszukując listę wcześniej zapisanych połączeń lub plików binarnych, można również wykryć ataki historyczne. Wyzwaniem często zgłoszonym przez organizacje próbujące wywiadu technicznego jest to, że sama ilość danych może szybko stać się przytłaczająca. W tym przypadku należy dokładnie rozważyć alokację zasobów, a organizacja może być bardziej selektywna w gromadzonych danych lub decydując się na budowę lub zakup dużych platform analitycznych, aby poradzić sobie z ilością danych. Ważne jest jednak, aby alokacja zasobów i rozwój zdolności były stale zbalansowane przed oceną korzyści płynących z wywiadu dotyczącego zagrożenia technicznego. Można by stwierdzić, że większe korzyści będą pochodzić z inwestowania w inne formy inteligencji. Istnieje wiele komentarzy w społeczności zabezpieczeń co do użyteczności technicznego rozpoznania zagrożeń, a niektóre twierdzą, że jest to bardzo skuteczny sposób zapobiegania i wykrywania kompromitacji, inni wątpią w jego użyteczność. Ta ostatnia grupa porównuje ją do sygnatur antywirusowych, ponieważ napastnicy mogą w niewielkim stopniu przystosować się, aby zapewnić, że ich narzędzia nie są rozpoznawane. Istnieje obawa, że duże ilości danych nie zawierają informacji kontekstowych, a zatem nie mogą dostarczyć większej analizy i oceny źródeł.
- **Taktyczne**: Rozpoznanie taktyczne może być jedną z najbardziej użytecznych form rozpoznania w zakresie ochrony organizacji. Jest to informacja dotycząca taktyki wykorzystywanej przez grupy napastników – w tym ich narzędzi i metodologii – i jest często określana jako



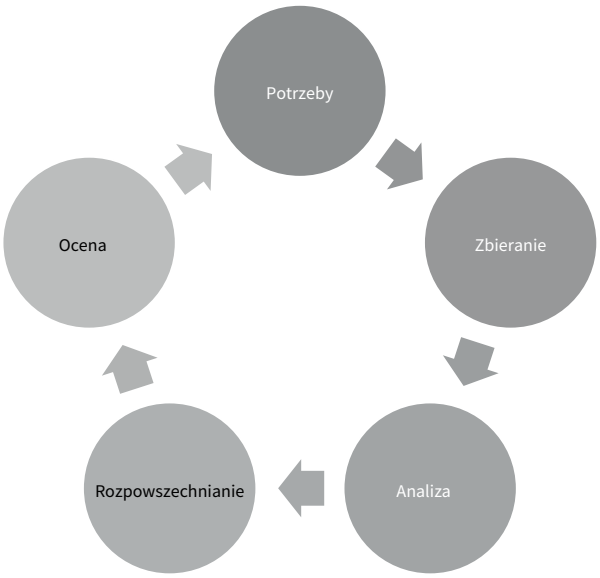
Rysunek 1. Schemat rozpoznania zagrożeń cybernetycznych
Źródło: Bank of England, 2016c, p. 13.

Taktyki, Techniki i Procedury (TTP – Tactics, Techniques and Procedures). Celem taktycznego rozpoznania zagrożeń jest zrozumienie, w jaki sposób aktorzy (*actors* – sprawcy) mogą atakować organizację, a także mapować tę wiedzę na sposoby, jak te ataki można złagodzić lub wykryć. Taktyczne rozpoznanie zagrożeń cybernetycznych jest wykorzystywane przez obrońców, takich jak architekci, administratorzy i personel ochrony. Źródłami informacji taktycznych są raporty o incydentach, atakach i kampaniach publikowane w Internecie, statyczna i dynamiczna analiza malware.

- **Operacyjne**: szczegółowa analiza poszczególnych ataków oraz określenie możliwości obrony na podobne zagrożenia w przyszłości. Operacyjne rozpoznanie zagrożeń to trafne informacje o konkretnych atakach przychodzących. Informuje o naturze ataku, tożsamości i zdolności atakującego – i wskazuje, kiedy może nastąpić atak. Służy do złagodzenia ataku: na przykład poprzez usunięcie ścieżek ataku lub utwardzenie systemu zabezpieczeń. Źródłem rozpoznania mogą być wszelakie socialmedia, fora dyskusyjne, źródła osobowe, grupy dyskusyjne,
- **Strategiczne**: wiedza o zmieniającym się ryzyku (strategicznych przesunięciach) konieczny jest ośrodek dowodzący do określenia krytycznej oceny zagrożeń. Strategiczne rozpoznanie zagrożenia jest przeznaczone dla kierownictwa wysokiego szczebla w organizacji, zazwyczaj zarząd lub osoby reprezentujące zarząd. Ma ona na celu pomóc strategom zrozumieć obecne zagrożenia oraz zidentyfikować dalsze zagrożenia, o których jeszcze



Rysunek 2. Rodzaje rozpoznania zagrożeń
Źródło: MWR Infosecurity, 2015.



Rysunek 3. Cykl rozpoznania
Źródło: (MWR Infosecurity, 2015).

nie są świadomi. Zajmuje się takimi pojęciami jak ryzyko i prawdopodobieństwo, a nie aspektami technicznymi, jest używany przez zarząd do prowadzenia strategicznych decyzji biznesowych i zrozumienia wpływu podejmowanych decyzji. Materialnie jest często w formie prozy, na przykład raportów lub briefingów – zarówno podczas konferencji, jak i spotkań indywidualnych z kadrą kierowniczą i członkami zarządu. Posiada silny biznesowy nacisk, który jest używany do prowadzenia strategii. Źródłami rozpoznania mogą być oceny sytuacji geopolitycznej (trendy, ambicje, strategie) analizy i raporty finansowe i giełdowe, polityczne kontakty międzyludzkie, artykuły publikowane w prasie autorstwa wysoko postawionych osób. Większość tych danych można odnaleźć stosując źródła o otwartym dostępie (OSINT).

Gartner – przedsiębiorstwo analityczno–doradcze specjalizujące się w zagadnieniach strategicznego wykorzystania technologii oraz zarządzania technologiami definiuje rozpoznanie zagrożeń jako wiedzy bazującej na dowodach, przy wykorzystaniu kontekstu, mechanizmów wskaźników, implikacji, zgłoszeń o powstających lub istniejących zagrożeniach. Kluczowymi wyzwaniami są: trudność w określeniu wskaźników ryzyka, kiedy nie znamy przeciwników i ich intencji, przygotowanie bezpieczeństwa powinno odbywać się na około trzy lata do przodu a nie tylko na istniejące zagrożenia (Gartner, 2014).

Bank of England twierdzi wręcz, iż testy penetracyjne tak często używane w celu podniesienia bezpieczeństwa, nie są już adekwatne do ochrony bezpieczeństwa sektora bankowego i zaleca ochronę instytucji finansowych w oparciu o rozpoznanie zagrożeń cybernetycznych (Bank of England, 2016a, pp. 21–22) (Bank of England, 2016b).

Efektywny program rozpoznania posiada kilka obszarów, na których można się skoncentrować. Podział rozpoznania zagrożeń na konkretne funkcje pozwala lepiej go skalować, gdyż poszczególni członkowie zespołu mogą być bardziej wykwalifikowani w określonych aspektach rozpoznania. Mogą skupić się i rozwijać na poszczególnych częściach cyklu, łatwiej też będzie śledzić konkretne słabości lub braki w poszczególnych etapach (MWR Infosecurity, 2015). Poszczególne etapy cyklu rozpoznania przedstawia rysunek 3:

- **Wymagania**: krok, który jest często pomijany, a może być kluczem do udanego programu. Kierownictwo musi określić, co chce wiedzieć konkretnie i co powinien im powiedzieć program rozpoznania zagrożeń. Na przykład wymóg może brzmieć następująco: „Informuj nas o wszystkich powszechnie znanych, powszechnie wykorzystywanych lukach w ciągu jednego dnia od ich poznania". Wymagania mogą być bardziej restrykcyjne dla zespołów rozpoznania zagrożeń, np. „Uzyskiwanie szczegółowych informacji i próbek większości narzędzi do zdalnego dostępu do zestawów przestępczych dla naszych zespołów ds. forensyki". Zespoły muszą współpracować z decydentami, aby uzgodnić wymogi, które są nie tylko możliwe do osiągnięcia, ale przede wszystkim dostarczą produktów, na których organizacja będzie mogła działać.
- **Zbieranie**: krok, który może dominować w znacznej części budżetu zespołu do rozpoznania zagrożeń cybernetycznych, polega na gromadzeniu informacji lub danych, które należy przeanalizować. Informacje mogą pochodzić z wielu różnych źródeł, takich jak kanały informacyjne, płatne usługi lub kanały, fora a nawet źródła ludzkie. Prawie wszystkie informacje o zagrożeniach wymagają jakiejś analizy. Zrozumienie, które źródła mogą generować pożądane informacje, które są wiarygodne i dostarczają wartościowych informacji i w jakim czasie je wykorzystać nie jest banalnym procesem.
- **Analiza**: przekształcanie danych w informacje, które mogą być później wykorzystane często wymaga analizy. W niektórych przypadkach analiza będzie stosunkowo prosta, np. przeanalizowanie pliku danych do zestawu reguł „deny" i alertów zapory. W innych przypadkach będzie wymagało wyodrębnienia odpowiednich informacji z większego zbioru, na przykład z raportu i zrozumienia, które elementy mają zastosowanie do aktywów organizacji. Ważną rolę dla analityka ma poszukiwanie możliwości tworzenia nowych typów inteligencji poprzez syntezę z bieżącej wersji. Na przykład analityk może poświęcić czas na czytanie dokumentów, aby wyodrębnić wskaźniki kompromisu, a także określić operacyjne informacje, które mogą być przekazane obrońcom sieci. Ewentualnie po przeczytaniu takich dokumentów i innych źródeł analityk może identyfikować trendy, które można zebrać razem w produkt strategiczny wywiadu dla wyższego zarządzania. Czasem okazuje się, że zebrane dane nie zawierają ważnych danych analitycznych i należy powrócić do etapu zbierania.
- **Produkcja/rozpowszechnianie**: na tym etapie tworzona jest i rozpowszechniana informacja o rozpoznaniu (wywiadowcza) dla klientów (kierownictwo, administratorzy sieci, obrońcy itp.). Informacja będzie się różnić w zależności od podtypu rozpoznania i klienta. Na przykład może wymagać od raportu, informacji dla obrońców lub po prostu zatwierdzonej reguły dodanej do sprzętu chroniącego sieć.
- **Ocena**: innym często zaniedbywanym etapem rozpoznania w sytuacjach zagrożenia jest ocena informacji w celu zapewnienia jej zgodności z pierwotnymi wymaganiami. Jeśli wymagania zostały zrealizowane, informacja może

dodatkowo spełniać wymogi, aby pomóc opracować nowe, głębsze wymagania, które opierają się na rozpoznaniu – a cykl wywiadowczy może się powtórzyć. Jeśli analiza zagrożeń nie spełnia wymagań, sugeruje w pewnym momencie awarię, to model cyklu można wykorzystać do ustalenia, gdzie wystąpiła awaria. Czy wymagania były nierealne? Czy proces zbierania używał złych źródeł? Czy dane zawarte w źródłach zostały pobrane, ale nie zostały wyciągnięte podczas analizy?

Korzyści ze stosowania rozpoznania zagrożeń cybernetycznych

INSA (Intelligence and National Security Alliance) stowarzyszenie środowisk wywiadowczych z siedzibą w Arlington zrzeszające byłych i obecnych pracowników NSA, CIA, Rady Bezpieczeństwa Narodowego, Narodowej Rady Wywiadu w swym raporcie wymienia główne zalety z taktycznego rozpoznania cybernetycznego (INSA, 2015, p. 3):

- Zapewnia kontekst i przydatność ogromnej ilości danych. Wiele organizacji posiada dostęp do terabajtów danych bez możliwości jej zrozumienia i filtrowania tak by uczynić je użytecznymi. Na poziomie taktycznym, kluczowe jest odfiltrowanie szumu. Taktyczne cyber–rozpoznanie wprowadza procesy metodyczne, które pomagają zarządzać przychodzącymi danymi, zamieniając je w cenną i praktyczną wiedzę o zagrożeniach.
- Pozwala organizacjom rozwijać proaktywną postawę i wzmocnić cyberbezpieczeństwo oraz ogólne zasady zarządzania ryzykiem. Rozpoznanie na poziomie taktycznym musi być wystarczająco precyzyjne, tak aby wspierać zdolność organizacji do zminimalizowania ryzyka. Poprzez identyfikację organizacyjnych i sieciowych podatności a także wzorów postępowania przeciwnika rozpoznanie cybernetyczne może zapewnić prawdopodobną drogę ataku, odsłaniając obszary najwyższego ryzyka określając słabości tak techniczne jak i organizacyjne.
- Pomaga podejmować lepsze decyzje w trakcie i po wykryciu cyberzagrożenia. Zgromadzona w systemie informacja o zagrożeniach i dzienniki zdarzeń (logi), może zapewnić pełniejszy obraz tego, jak przeciwnik zyskał lub próbuje zdobyć dostęp do organizacji. Wskaźniki kompromitacji (IOCs) obejmujące sygnatury wirusów oraz pliki malware, adresy IP i inne wskazówki nieprawidłowej aktywności sieciowej, które mogą pomóc ujawnić TTP (Taktyki, Techniki i Procedury) przeciwnika, a także, jakie dane mogły zostać przejęte. Wskaźniki kompromitacji mogą ujawnić kim jest przeciwnik, jakie może mieć intencje i motywacje.
- Ukierunkowuje cyberbezpieczeństwo na tor proaktywny, z możliwością przewidywania następnych ataków, a nie tylko reaktywny, reagujący po zaistniałym fakcie. Większa ilość zgromadzonych analiz i danych pozwoli organizacji na zapewnienie lepszej obrony i doskonalenie technik rozpoznania cybernetycznego.

Wobec wyrafinowanych i bezwzględnych „cyberprzeciwników", organizacje muszą ciągle doskonalić swoje zdolności obronne. Mogą zatrudnić zespoły zdolnych obrońców sieci komputerowej, ale nawet najbardziej elitarni eksperci mogą nie być w stanie zabezpieczyć „cybergranic" bez użycia równie sprawnych narzędzi.

To czego potrzebują to platforma do przechowywania bardzo szczegółowych informacji na temat każdego indywidualnego zagrożenia. Potrzebują także instrumentów do wykonywania zaawansowanych analiz tych danych do tworzenia swoistych informacji wywiadowczych. I muszą być w stanie udostępniać te informacje na bieżąco wśród członków zespołu obrony, tak aby zapobiec następnym atakom cybernetycznym, zanim one nastąpią, a nie już po stwierdzonym fakcie.

Źródła rozpoznania zagrożeń cybernetycznych

- Wewnętrze – źródła wewnętrzne to wszystkie informacje zbierane wewnątrz organizacji. Najczęściej to informacje gromadzone przez firewalle, systemy zapobiegania włamaniom (IPS), systemy zabezpieczeń, antywirusy, dzienniki zdarzeń systemów, czyli większość informacji wewnętrznej bierzemy z sieci organizacji. Cenną informacją są analizy powłamaniowe komputerów i odnalezione w nich cyfrowe dowody. Pełna dogłębna analiza pozwala zidentyfikować narzędzia bądź taktykę, technikę i procedury (TTP) atakujących, które nie zmieniają się tak często jak adresy czy domeny.
- Społecznościowe – ta kategoria obejmuje każdą społeczność dzieląca się informacjami o rozpoznaniu zagrożeń, która posiada relacje zaufania i wspólne interesy. Może być to także nieformalna grupa np. przedsiębiorców reprezentujących tę sama gałąź przemysłu lub zrzeszenie wyższych uczelni.
- Zewnętrzne – kategoria ta zawiera wszystkie informacje zdobywane spoza własnej organizacji lub od zaufanych partnerów. Istnieją dwa typy źródeł zewnętrznych. Pierwszym z nich są źródła publiczne. Źródła te są dostępne dla każdego i zwykle są bezpłatne. Brak kosztów ponoszonych za dostęp do tych źródeł może wiązać się z brakiem gwarancji dostępu to tychże usług. Istnieje wiele takich baz w sieci udostępniających adresy IP, domeny, skróty niebezpiecznych plików, w różnych formatach, często po uprzedniej rejestracji (SANS Institute, 2013, pp. 9–10), (Liska, 2015). ■

Bibliografia

1. ActiveResponse.org, 2016. *The Diamond Model.* [Online] Available at: http://www.activeresponse.org/the-diamond-model/ [Data uzyskania dostępu: 13 marzec 2017].
2. Bank of England, 2016a. *An Introduction to Cyber Threat Modelling v2.0*, Londyn: BANK of England.
3. Bank of England, 2016b. *CBEST Implementation Guide*, Londyn: Bank of England.
4. Bank of England, 2016c. *CBEST Intelligence-Led Testing*, Londyn: Bank of England.
5. Caltagirone, S., Pendergast, A. i Betz, C., 2013. *The Diamond Model of Intrusion Analysis*, Hanover, MD: Center for Cyber Threat Intelligence and Threat Research.
6. ENISA, 2014. *ENISA Threat Landscape 2014*, Heraklion, Grecja: European Union Agency for Network and Information Security.
7. Gartner, 2014. *Threat intelligence what is it, and How Can it Protect You from Today's Advanced Cyber-Attack*, Broomfield: Webroot.
8. Hutchins, E. M., Cloppert, M. i Amin, R., 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, brak miejsca: Lockheed Martin.
9. INSA, 2015. *TACTICAL CYBER INTELLIGENCE*, Arlington: INTELLIGENCE AND NATIONAL SECURITY ALLIANCE.
10. Liska, A., 2015. *Building an Intelligence-led Security Program*. Waltham: Syngress.
11. MWR Infosecurity, 2015. *Threat Intelligence: Collecting, Analysing, Evaluating*, Londyn: MWR InfoSecurity.
12. National Cyber Security Centre, 2015. *An introduction to threat intelligence*, Londyn: CERT-UK Publication.
13. SANS Institute, 2013. *Tools and Standards for Cyber Threat Intelligence*, brak miejsca: SANS Institute.
14. SecureWorks, 2016. *Breaking the Kill Chain*, brak miejsca: SecureWorks.

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

BEZPIECZEŃSTWO POŻAROWE SYSTEMÓW FOTOWOLTAICZNYCH

Norbert Tuśnio

Instalacje fotowoltaiczne od kilku lat zagościły na naszych dachach. Społeczeństwo zainteresowane odnawialnymi źródłami energii podjęło ekonomiczną, w perspektywie kilkunastu lat decyzję, instalując panele. Ich niepodważalną zaletę można ująć w kilku słowach, jako obniżenie kosztów energii elektrycznej, a niedoskonałości i wątpliwości wymieniono poniżej:

- wieloletni czas oczekiwania na zwrot kosztów, szczególnie przy kredytowaniu inwestycji
- bliżej nieokreślony sposób utylizacji i recyklingu zużytych paneli oraz
- dodatkowe zagrożenie pożarowe od instalacji elektrycznej

Do tego systemy fotowoltaiczne nadal nie zapewniają skutecznego magazynowania energii, co dało się odczuć podczas ostatnich wichur w lutym w Polsce (tysiące odbiorców pozostało bez prądu nawet przez dwa dni). Natomiast w styczniu zerwała się konstrukcja paneli fotowoltaicznych z dachu firmy w Białymstoku. Podsumowując dywagację o alternatywnych źródłach energii należy dodać, że stoimy przed perspektywą budowy elektrowni atomowych w naszym kraju (co do tej pory się nie udało), ale jak mówi Krzysztof Broszkowski – Manager w Dziale Operacyjnym firmy FG Energy, nawet jeśli prąd będzie pochodził z elektrowni jądrowej, to nie spowoduje to nagłego spadku cen energii elektrycznej, a jedynie „uniezależnienie się" od sieci krajowych dystrybutorów i produkcja „własnego" prądu pozwoli na oszczędności w domowym budżecie. Instalacja paneli słonecznych jest szczególnie zalecana przy dużych poborach prądu (klimatyzacja, sauna) i w kombinacji z innymi OZE (np. pompą ciepła).

Wprowadzenie

Zadaniem instalacji fotowoltaicznych jest przetwarzanie energii słońca bezpośrednio w energię elektryczną. Jest to jeden z przykładów odnawialnych źródeł energii (OZE).

Wyróżnia się trzy podstawowe typy instalacji fotowoltaicznych:

- on-grid – instalacja podłączona do sieci elektroenergetycznej
- off-grid – instalacja niepodłączona do sieci elektroenergetycznej, co wymaga magazynowania energii
- hybrydowa – instalacja łącząca w sobie rozwiązania z on-grid oraz off-grid, z możliwością przyłączenia innych źródeł energii z grupy OZE

Z uwagi na charakter budowy i pracy, instalacja PV może w stanach awaryjnych stanowić zagrożenie porażeniowe dla ludzi.

Instalacja fotowoltaiczna pracuje zarówno podczas dziennego oświetlenia, jak i (w niepełnym zakresie) w warunkach ograniczonego oświetlenia (np. sztucznego). Pomimo iż ryzyko porażenia jest niewielkie, nie da się go całkowicie wyeliminować.

Instalację fotowoltaiczną (PV, ang. photovoltaic) można podzielić na część stałoprądową (panel-falownik) oraz zmiennoprądową (falownik-instalacja elektryczna w budynku).

Podczas prowadzonych działań ratowniczych strażacy muszą mieć na uwadze różnorodne zagrożenia, których nie sposób jest wymienić w jednym opracowaniu. Biorąc to pod uwagę, podczas formułowania zamiarów taktycznych, trzeba mieć zawsze na uwadze przede wszystkim bezpieczeństwo ekip ratowniczych.

Zasada działania instalacji fotowoltaicznej

1. Moduły fotowoltaiczne

Głównym składnikiem takiej instalacji są moduły fotowoltaiczne (rys. 1). Są to urządzenia elektryczne, w których przy wykorzystaniu zjawiska fotoelektrycznego zachodzi bezpośrednia przemiana energii promieniowania świetlnego (naturalnego lub sztucznego) w energię elektryczną. Każdy moduł fotowoltaiczny zbudowany jest z ogniw fotowoltaicznych, które połączone są ze sobą szeregowo lub szeregowo-równolegle. Całość jest odpowiednio zabezpieczona i umieszczona w obudowie tworzącej moduł (rys. 2). Napięcie znamionowe instalacji PV, np. o mocy 400 W, wynosi do 50 V. Sprawność modułu silnie zależy od natężenia promieniowania słonecznego. W celu uzyskania większych mocy moduły PV łączy się ze sobą szeregowo lub równolegle. Połączenie szeregowe powoduje wzrost napięcia w obwodzie DC (prądu stałego) proporcjonalnie do liczby połączonych modułów. Tak spięte moduły tworzą łańcuchy (stringi), z których energia elektryczna przekazywana jest za pomocą połączeń kablowych do falowników (inwerterów). Moduły fotowoltaiczne połączone wzajemnie ze sobą tworzą panel PV.

2. Falownik (ang. inverter)

Falownik (rys. 3) to urządzenie przekształcające energię elektryczną z prądu i napięcia stałego na energię w postaci prądu i napięcia przemiennego, zgodnego z wymaganymi parametrami sieci elektrycznej (w Polsce 230/400 V, 50 Hz). Falowniki dobiera się indywidualnie do potrzeb danej instalacji, uwzględniając przy tym m.in. wielkość instalacji i sposób pracy. Falownik może być zainstalowany w różnych miejscach (na zewnątrz i wewnątrz obiektu), które spełnia wymogi jego montażu podane przez producenta. Falownik nie tylko przetwarza energię elektryczną, ale jednocześnie realizuje następujące zadania:

- utrzymuje parametry prądu elektrycznego zgodne z wymogami publicznej sieci energetycznej
- monitoruje w sposób ciągły parametry pracy instalacji
- automatycznie odłącza system od sieci w przypadku zaniku napięcia prądu przemiennego AC

Uwaga! Nadal na odcinku między falownikiem a modułami może występować napięcie DC.

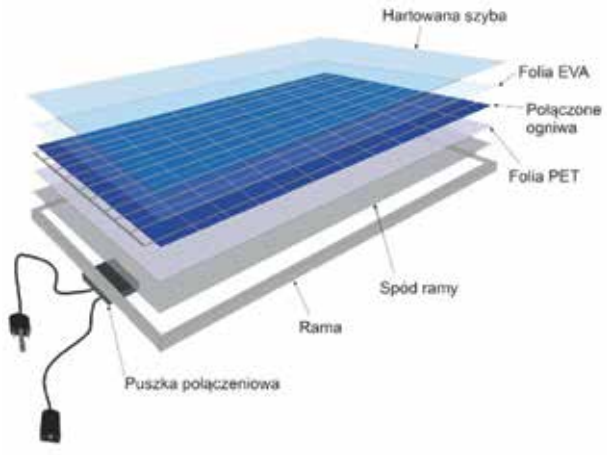
Innym stosowanym rozwiązaniem są mikrofalowniki (rys. 4) zwane również mikroinwerterami. Różnica w stosunku do falowników polega na tym, że są one bezpośrednio przyłączone do każdego pojedynczego modułu PV, z którego konwertują prąd stały (DC) na prąd przemienny (AC). Z uwagi na wskazanie montażu mikrofalownika do modułów, ich liczba w instalacji może wynosić od jednego do nawet kilkudziesięciu sztuk, przy założeniu maksymalnie jednego mikrofalownika na cztery moduły. Jedną z korzyści ich stosowania jest obniżenie napięcia po stronie DC do wartości bezpiecznej.

3. Okablowanie

Do prawidłowej pracy instalacji PV powinny być stosowane przewody specjalne tzw. solarne. Stałoprądowa część instalacji PV (na odcinku panel-falownik) prowadzona jest przewodami w podwójnej izolacji odpornej na promieniowanie UV i wpływ warunków atmosferycznych. W dużych instalacjach stosuje się kable jednożyłowe o przekroju od 4 mm^2 do 120 mm^2. Zabronione jest stosowanie „zwykłych" przewodów użytkowanych w instalacjach elektrycznych 230 V.

Zaleca się aby przewody prowadzone były w rurach, kanałach kablowych, zlokalizowanych wewnątrz lub na zewnątrz obiektu budowlanego. W praktyce zdarza się, że trasy kablowe prowadzone są ciągami wentylacyjnymi, co jest niezgodne z przepisami ochrony przeciwpożarowej.

Przewody prądu stałego (DC) łączy się ze sobą za pomocą konektorów (złączek) dedykowanych do instalacji PV (rys. 5). Obecnie spotykanym standardem są konektory typu MC4. Jednakże nie wszyscy producenci używają oryginalnych złączy, lecz złącza z nimi kompatybilne, o zbliżonej budowie. Niestety występowały przypadki, w których słabej jakości złącza pękały podczas montażu lub mrozów. Powodowało to zmniejszenie powierzchni styków lub siły docisku co prowadziło do wydzielania się nadmiernej ilości ciepła czy powstania łuku elektrycznego, na skutek wzrostu wartości rezystancji.



Rys. 1. Budowa modułu fotowoltaicznego
Źródło: https://poradnikprojektanta.pl/ogniwa-i-moduly-fotowoltaiczne-zasada-dzialania-i-budowa/

Rys. 2. Widok przedniej i tylnej części modułu fotowoltaicznego
Źródło: materiał firmy FG Energy

Rys. 3. Przykładowy falownik PV
Źródło: materiał firmy FG Energy

Rys. 4. Przykładowy mikrofalownik
Źródło: https://www.hoymiles.com/pl-eu/microinverter-single-phase/

4. Zabezpieczenia

Jedną z ważniejszych części instalacji fotowoltaicznych są urządzenia zabezpieczające i kontrolujące. Należą do nich zabezpieczenia nadmiarowo-prądowe (bezpieczniki, wyłączniki), rozłączniki, ograniczniki przepięć. Falownik, z uwagi na charakter swojej pracy, może również pełnić funkcje zabezpieczające.

W niektórych, z reguły bardziej rozbudowanych instalacjach fotowoltaicznych, spotyka się dodatkowe formy zabezpieczeń, np. optymalizatory mocy (rys. 6). Montowane są one pod modułami PV, poza swoim podstawowym przeznaczeniem polegającym na zoptymalizowaniu sprawności modułów, w razie awarii lub rozłączenia systemu PV, posiadają dodatkową funkcję zmniejszenia napięcia DC na modułach i przewodach do bezpiecznego poziomu. Uruchamiają się w momencie zaniku napięcia zasilającego lub odłączenia falownika, automatycznie zmniejszając napięcie modułów do 1 V. Dodatkowo falownik i optymalizator wyłączą się pod wpływem ekstremalnie wysokiej temperatury lub gdy wystąpi łuk elektryczny.

Rozłączniki bezpieczeństwa (rys. 7) – są urządzeniami służącymi do załączania i rozłączania napięcia stałego pochodzącego z modułów fotowoltaicznych. Ich sterowanie odbywa się automatycznie poprzez sieć prądu przemiennego. Celem ich działania jest rozłączenie obwodu prądu stałego w momencie przerwy w zasilaniu po stronie prądu przemiennego i automatyczne załączenie obwodu prądu stałego po przywróceniu zasilania prądu przemiennego. Taka sytuacja następuje w przypadku awarii sieci energetycznej lub umyślnego wyłączenia zasilania budynku, gdy istnieje zagrożenie pożarowe. Rozłączniki automatyczne nie wymagają obsługi, a dzięki umiejscowieniu ich w pobliżu modułów, dają dodatkową korzyść, polegającą na obniżeniu napięcia na trasach kablowych po stronie DC.

Rys. 5. Konektor typ MC-4
Źródło: https://www.semicon.com.pl/dlaczego-warto-wybrac-oryginalne-zlacza-mc4/

5. Dodatkowe wyposażenie instalacji PV

Do dodatkowego wyposażenia instalacji fotowoltaicznej należą:

- magazyn energii – stałoprądowy bank energii zwykle wykonany na bazie baterii akumulatorów. Mogą one tworzyć system połączonych ze sobą szeregowo-równolegle baterii o całkowitej pojemności kilkuset Ah przy różnym napięciu sięgającym nawet 48 V (stanowią kluczowy element większości instalacji off-grid)
- regulator ładowania – służący do kontrolowania procesu ładowania magazynów energii w systemach fotowoltaicznych (chroni baterie przed przeładowaniem oraz nadmiernym rozładowaniem, a w konsekwencji przed ich uszkodzeniem)

Zagrożenia występujące przy pracy w obrębie systemów fotowoltaicznych

Do zagrożeń związanych z pracą w pobliżu systemów fotowoltaicznych należą:

- Ryzyko porażenia łukiem elektrycznym. Łuk elektryczny powstaje zwykle przy rozłączaniu obwodów pod napięciem. Przykładowo, uderzenie toporem strażackim w przewód zasilający pracującej instalacji fotowoltaicznej mogłoby spowodować powstanie łuku elektrycznego pomiędzy biegunami dodatnim i ujemnym. Z tego powodu niszczenie przewodów zasilających jest zabronione. Należy również pamiętać, że nawet po przecięciu przewodu zasilającego, fragment od panelu do miejsca przecięcia nadal znajduje się pod napięciem.

Rys. 6. Optymalizator mocy
Źródło: materiał firmy FG Energy

Rys. 7. Rozłącznik bezpieczeństwa DC
Źródło: materiał firmy FG Energy

- Ryzyko upadku z wysokości.
- Spadające elementy z dachu. Podczas prowadzenia działań w obrębie instalacji PV należy liczyć się ze spadającymi jej fragmentami, co jest szczególnie prawdopodobne w przypadku pożarów obejmujących pionowo zamontowane panele (np. na elewacji budynku).
- Ryzyko poparzenia.
- Występowanie gazów toksycznych w trakcie spalania elementów instalacji. Ogniwa fotowoltaiczne w trakcie spalania wytwarzają trzy główne szkodliwe związki chemiczne, takie jak: rakotwórczy tellurek kadmu CdTe (zwykle w instalacjach komercyjnych lub użytkowych), arsenek galu GaAs (wysoce toksyczny i rakotwórczy), fosfor P (dawka śmiertelna wynosi 50 mg), czy chlorowodór HCl powstały podczas topienia się izolacji przewodów (wysoce toksyczny, w reakcji z wodą tworzy kwas solny).
- Ryzyko porażenia prądem podczas prac rozbiórkowych szczególnie w systemach z potencjalnymi awariami i uszkodzonymi komponentami – niezależenie od odłączenia zasilania obiektu, część instalacji od modułu fotowoltaicznego do falownika może znajdować się pod napięciem, nawet podczas działań po zmierzchu, w przypadku oddziaływania takich źródeł światła jak: księżyc w pełni, płomień, sztuczne oświetlenie miejsca prowadzenia działań.
- Ryzyko wystąpienia napięcia na konstrukcji montażowej. Należy pamiętać, że nawet jeden uszkodzony element instalacji taki jak moduł, konektor, przewód może spowodować pojawienie się napięcia na metalowych elementach przewodzących obiektu i instalacji.

Porażenie prądem elektrycznym

Porażenie prądem elektrycznym jest jednym z zagrożeń typowych w służbie pożarniczej. Powszechność użytkowania energii elektrycznej, a także nowoczesne technologie, na czele z rozwijającą się elektromobilnością i stale rosnącym udziale instalacji fotowoltaicznych, stwarzają wyzwanie dla służb ratowniczych. Obiekt pod napięciem to fragment instalacji lub urządzenia elektrycznego, którego cechuje potencjał elektryczny wyższy niż potencjał ziemi, przyjmowany jako 0 V. W niektórych sytuacjach, np. izolowanych od ziemi układach zasilania, różnica potencjałów występuje pomiędzy biegunami źródła napięcia. Z praktycznego punktu widzenia oznacza to, że jeżeli obiekt pod napięciem zostanie uziemiony, np. poprzez dotknięcie dłonią, nastąpi przepływ prądu rażeniowego przez ciało człowieka do ziemi. Innymi słowy, człowiek stanie się częścią obwodu elektrycznego. Należy pamiętać, że napięcie jest zawsze przyczyną, a przepływ prądu skutkiem. A zatem czym wyższe napięcie obiektu, tym większy prąd przepłynie przez ciało człowieka. Należy również podkreślić, że jeżeli człowiek będzie skutecznie odizolowany od ziemi (np. poprzez obuwie dielektryczne), dotknięcie obiektu pod napięciem nie spowoduje porażenia. Sprawi to jedynie, że człowiek będzie znajdował się pod napięciem. Co do zasady, czym wyższe napięcie obiektu, tym skutki porażenia mogą być groźniejsze.

Po dotknięciu obiektu pod napięciem, rezystancja ciała człowieka oraz posiadanych środków ochrony indywidualnej (obuwie, rękawice) będzie wpływać na wartość prądu rażenowego. Wartość ta, z kolei, przyczynia się do skutków porażenia odniesionych bezpośrednio do organizmu strażaka. Prąd elektryczny przepływający przez żywy organizm wywołuje w nim różne zmiany fizyczne, chemiczne oraz biologiczne.

Na skutki porażenia prądem elektrycznym wpływają następujące czynniki:

- elektryczne (rodzaj, wielkość natężenia, czas przepływu prądu)
- fizjologiczne (stopień rozwoju organizmu człowieka, stan naskórka)
- zewnętrzne (czynniki wpływające na zmniejszenie rezystancji ciała ludzkiego, np. wilgotność, wysoka temperatura)

Zgodnie z obowiązującymi normami, za próg wyczuwalności uznaje się wartość prądu 0,5 mA. Należy pamiętać, że jest to wartość dużo niższa od typowych prądów znamionowych domowych instalacji elektrycznych (np. 16 czy 25 A). Już taka wartość natężenia prądu stanowi zagrożenie wystąpienia niekontrolowanych odruchów.

Skutki porażenia prądem

Warto podkreślić, że poza zakłócaniem naturalnych dla organizmu sygnałów elektrycznych przekazywanych przez układ nerwowy, istota porażenia prądem wiąże się z wydzielaniem ciepła od rezystancji tkanek, wzrostu ich temperatury i niszczeniem struktur biologicznych. Dlatego prąd elektryczny może oddziaływać na organizm ludzki w sposób pośredni lub bezpośredni. Działanie pośrednie powstające bez przepływu prądu przez ciało człowieka, powoduje takie urazy jak:

- oparzenia ciała wskutek pożarów wywołanych zwarciem elektrycznym lub spowodowane dotknięciem do nagrzanych elementów
- groźne dla życia oparzenia ciała łukiem elektrycznym, a także metalizacja skóry spowodowana osadzaniem się roztopionych cząstek metalu

- uszkodzenia wzroku wskutek dużej jaskrawości łuku elektrycznego
- uszkodzenia mechaniczne ciała w wyniku upadku z wysokości lub upuszczenia trzymanego przedmiotu

Uwaga! Tradycyjne systemy PV pracują pod napięciem do 1000 V DC.

Potencjalne przyczyny pożarów instalacji fotowoltaicznych

Systemy fotowoltaiczne stale sprawdzają się jako jedne z najbardziej preferowanych źródeł alternatywnej energii, a rocznie (dane na 2019 r.) instaluje się panele o łącznej mocy ponad 120 GW. Systemy fotowoltaiczne są wyjątkowo bezpieczne w normalnych warunkach pracy, jeśli są instalowane i konserwowane przez profesjonalistów zgodnie z przepisami i wytycznymi dotyczącymi instalacji elektrycznych. Jednak wraz z rosnącą dystrybucją różnych systemów fotowoltaicznych działających zarówno na ziemi, na dachach, a nawet zintegrowanych z budynkami, należy wziąć pod uwagę ryzyko możliwego pożaru w miejscu instalacji systemów fotowoltaicznych (tak jak w przypadku każdej sieci energetycznej).

W latach 1995–2012 w Niemczech zgłoszono 400 pożarów związanych z systemami fotowoltaicznymi. W 180 przypadkach źródłem pożaru był pojedynczy element fotowoltaiczny. Aby podkreślić bezpieczeństwo systemów fotowoltaicznych, należy wspomnieć, że te 180 przypadków stanowiło mniej niż 0,1% wszystkich pożarów w Niemczech w tym okresie. Jednym z przykładów tego typu pożarów w tym kraju był pożar w fabryce w Norderney w sierpniu 2013 r. (spowodował szkody wynoszące miliony euro).

Różne elementy systemu fotowoltaicznego są palne ze względu na zawartość polimerów, na przykład: folia do enkapsulacji EVA (ang. ethylene vinyl acetate) i polimerowa warstwa tylna w modułach, polimery w kablach, puszkach połączeniowych i falownikach. Badania prowadzone przez niemieckie Federalne Ministerstwo Gospodarki i Technologii wykazały, że w przypadku systemu o mocy 9 kWp (jednostka ta nie dorobiła się jeszcze swojego polskiego odpowiednika) z 38 standardowymi modułami fotowoltaicznymi jest do 60 kg materiału polimerowego z samych modułów. Polimery mogą wytwarzać podwyższoną temperaturę porównywalną z temperaturą oleju opałowego. Ciepło spalania polietylenu (46 MJ/kg) jest nawet wyższe niż oleju opałowego (43 MJ/kg).

Podczas pożaru i bezpośrednio po nim, system fotowoltaiczny może potencjalnie emitować szkodliwe związki w postaci cieczy, ciał stałych lub dymu. Sami użytkownicy mogą czuć się bezpiecznie wobec toksycznych produktów spalania ze względu na niewielką ilość niebezpiecznych substancji występujących w systemach fotowoltaicznych. Jednak strażacy interweniujący w zdarzeniu mogą być narażeni na niebezpieczne poziomy stężeń metali, takich jak ołów, kadm i selen, jeśli w systemie znajdują się moduły cienkowarstwowe.

Jak zmniejszyć to zagrożenie?

Strażacy muszą być poinformowani o istnieniu modułów fotowoltaicznych, ich lokalizacji i rodzaju, aby odpowiednio i bezpiecznie zaplanować swoje działania.

Strażacy muszą używać masek, aby chronić się przed szkodliwym i potencjalnie toksycznym gazem.

Odpady z uszkodzonego miejsca instalacji fotowoltaicznej wymagają profesjonalnej utylizacji.

Ograniczenie przestrzeni na dachu po instalacji systemu PV utrudnia dostęp i może powodować poślizgnięcie czy upadek z wysokości.

Jak „pomóc” strażakom?

Należy zachować przejścia o określonej szerokości i odpowiednie odstępy od granic dachu.

Należy oznaczyć przewody prądu stałego i zachować aktualny schemat układu okablowania.

Urządzenia fotowoltaiczne zwiększają obciążenie dachu, co może prowadzić do potencjalnego zawalenia się dachu w czasie pożaru. Zagrożenie to rośnie, jeśli belki nośne zostaną osłabione z powodu działania ognia i wysokiej temperatury. Moduły także mogą spaść na ziemię podczas pożaru, zagrażając zarówno mieszkańcom, jak i ratownikom.

Ostatecznie należy:

- Zachować poprawność techniczną podczas procesu projektowania, ewentualnie skonsultować się z inżynierem budowlanym.
- W przypadku wzywania straży pożarnej, poinformować o obecności na dachu systemu fotowoltaicznego.

Systemy fotowoltaiczne mają wysokie napięcie DC, które potencjalnie może wytworzyć łuk w przypadku wystąpienia awarii. Może on trwać do momentu wyłączenia napięcia lub zwiększenia odległości między stykami.

Powodem łuków elektrycznych mogą być źle przylutowane złącza ogniw lub nieprawidłowe połączenia między złączami ogniw a szynami zbiorczymi wewnątrz modułu.

Niskiej jakości puszki połączeniowe z niepewnymi stykami przewodów i nieutrzymujące szczelności mogą prowadzić do korozji, słabego odprowadzania ciepła, a niskiej jakości bypassy mogą również powodować zwarcia łukowe.

Inne ryzyko może powstać w przypadku stosowania złączy dwóch różnych producentów.

Opór przejścia elektrycznego może znacznie wzrosnąć, powodując intensywne nagrzewanie się uszkodzonego elementu.

Jak temu zapobiec?

Należy wybierać tylko wysokiej jakości komponenty systemu fotowoltaicznego, takie jak moduły fotowoltaiczne, kable, falowniki. Nie należy jednocześnie stosować złączy różnych producentów.

Moduły fotowoltaiczne wytwarzają energię tak długo, jak są wystawione na wystarczająco silne źródło światła. Nawet sztuczne źródła światła z lamp halogenowych mogą wytwarzać wystarczającą moc do zasilania systemów fotowoltaicznych do niebezpiecznego poziomu. To samo zagrożenie może powstać od światła pochodzącego z płomieni.

W raporcie UL (ang. Underwriters Laboratories) dotyczącym bezpieczeństwa strażaków i systemów fotowoltaicznych (dostępnym na stronie CESA, ang. Clean Energy States Alliance) zgromadzono zalecenia dotyczące bezpieczeństwa pożarowego systemów PV.

Zgodnie z polskimi przepisami konieczne prace wyburzeniowe i rozbiórkowe wykonywane są tylko w okolicznościach uzasadnionych stanem wyższej konieczności (prawo ich zarządzenia ma strażak kierujący akcją ratowniczą). W takich okolicznościach kierujący akcją może posłużyć się prawem odstąpienia od zasad działania uznanych powszechnie za bezpieczne. Potencjalne ryzyko dla strażaka stanowi potrzeba otworzenia dachu, aby uzyskać dostęp do systemu fotowoltaicznego. Oznacza to niekiedy konieczność przecięcia przewodów pod napięciem – jest to element działania ratowniczego, który prawie zawsze powoduje wytworzenie łuku i może stanowić znaczne zagrożenie niebezpiecznego porażenia prądem. Cięcie okablowania paneli słonecznych pod napięciem musi więc przebiegać w sposób profesjonalny.

Nawet uszkodzone moduły mogą nadal wytwarzać energię, która może zagrażać strażakom-ratownikom podczas demontażu i składowania. Test UL pokazał, że nawet po uszkodzeniu spowodowanym przez ciepło lub ogień, 60% modułów może nadal działać z pełną mocą.

Jak sobie z tym radzić?

Odłączyć zasilanie systemu fotowoltaicznego.

Strażacy muszą być wyposażeni w aparaty ochrony dróg oddechowych.

Należy uruchomić procedurę szybkiego wyłączenia, aby wyeliminować ryzyko bezpośredniego kontaktu strażaków z przewodem prądu stałego pod napięciem.

Uwaga! Szybkie wyłączenie (ang. Rapid Shutdown) zostało wprowadzone w Stanach Zjednoczonych w celu zmniejszenia liczby pożarów i poprawy bezpieczeństwa strażaków gaszących systemy fotowoltaiczne.

Szybkie wyłączanie zostało po raz pierwszy wprowadzone w Narodowym Kodeksie Elektrycznym (NEC) z 2014 r., aby zapewnić strażakom prostą metodę łatwego odłączania przewodów prądu stałego instalacji słonecznej w celu zapewnienia bezpiecznych działań na dachu budynku podczas pożaru. W standardowym układzie PV z falownikiem, nawet gdy jest on wyłączony, okablowanie DC z układu słonecznego pozostaje pod napięciem przy słonecznej pogodzie.

W Stanach Zjednoczonych, zgodnie z sekcją 690.12 National Electric Code 2017, napięcie prądu stałego na przewodach modułu musi być niższe niż 80 V po czasie 30 sekund od szybkiego wyłączenia.

W Niemczech norma VDE-AR-E 2100-712 dopuszcza napięcie nie większe niż 120 V w całym generatorze fotowoltaicznym po wyłączeniu.

Dzięki dalej opisanym rozwiązaniom instalatorzy mogą spełnić nawet najbardziej rygorystyczny standard.

Urządzenie Santon switch można zainstalować w pobliżu ciągów fotowoltaicznych. W przypadku pożaru, gdy strażak wyłącza obwód prądu przemiennego, wyłącznik ten bezpośrednio odłącza prąd stały w bezpośredniej bliskości modułów słonecznych, co sprawia, że miejsce to jest znacznie bezpieczniejsze dla strażaków. Wyłącznik przeciwpożarowy prądu DFS zachowa się w ten sam sposób, jeśli temperatura wzrośnie powyżej 100°C. Po powrocie zasilania prądem zmiennym urządzenie DFS automatycznie włącza zasilanie prądem stałym.

SolarEdge jest jednym z niewielu producentów sprzętu solarnego, który zapewnia zintegrowaną funkcję szybkiego wyłączania. W przypadku zastosowania jednej z poniższych metod napięcie ciągu zostanie zredukowane do równej liczby modułów w ciągu (jeśli w ciągu jest 30 modułów, to w czasie 30 s napięcie ciągu wynosi 30 V):

- Wyłącznik AC falownika jest wyłączony lub napięcie AC do falownika jest odłączone inną metodą (celowo lub w wyniku błędu)
- Przełącznik ON/OFF falownika jest wyłączony
- Wyłącznik prądu DC jest wyłączony (dotyczy tylko inwerterów z modułem bezpieczeństwa)

Istnieją dwa sposoby spełnienia wymagań NEC 690.12 w zakresie szybkiego wyłączenia (Rapid Shutdown):

- Produkty Tigo Flex MLPE (ang. Module Level Power Electronics) wykorzystują bezprzewodową komunikację między elektroniką modułu TAP i TS4. Flex MLPE wymaga TAP (ang. Tigo Access Point) i CCA (ang. Cloud Connect Advanced) w celu szybkiego wyłączenia.
- Transmiter TS4-F wykorzystuje komunikację PLC i nadajnik RSS. TS4-F wykonuje tylko szybkie wyłączanie bez monitorowania na poziomie modułu.

Oba rozwiązania można zastosować do wszystkich głównych falowników i modułów fotowoltaicznych. W sytuacjach awaryjnych, takich jak pożar, standardową procedurą dla ratowników pierwszego rzutu jest odłączenie wyłącznika obwodu prądu przemiennego w budynku. Ta utrata zasilania z sieci powoduje wyłączenie falownika i modułu Cloud Connect Advanced (CCA) lub nadajnika RSS. Za każdym razem, gdy CCA lub RSS wyłącza się, jednostki TS4 służące do zapewnienia bezpieczeństwa (TS4-S, TS4-O, TS4-L i TS4-F) automatycznie wchodzą w tryb odłączenia na poziomie modułu i całkowicie wyłączają napięcie wyjściowe i zasilanie. Tak więc, nawet jeśli ekipa ratownicza nie aktywuje bezpośrednio odłączenia poziomu modułu, jednostki TS4 są przystosowane do uruchomienia standardowego protokołu bezpieczeństwa i reagowania na sytuacje kryzysowe. Ta sama koncepcja dotyczy systemu opartego na TS4-F. Jeśli używane są zewnętrzne nadajniki RSS, należy je wyłączyć w tym samym czasie, co falownik, aby spełnić wymagania NEC 690.12.

Zakończenie

Problem bezpieczeństwa pożarowego systemów fotowoltaicznych został od początku dostrzeżony przez krajowe służby ratownicze z Komendą Główną Państwowej Straży Pożarnej na czele. Dlatego wiele informacji, które znalazły się w opracowaniu, zaczerpniętych zostało z niezatwierdzonej jeszcze procedury „Standardowe zasady postępowania podczas zdarzeń w obrębie instalacji fotowoltaicznych". Jest to kolejny zbiór dobrych praktyk po opublikowanych „Standardowych zasadach postępowania podczas zdarzeń z samochodami osobowymi z napędem elektrycznym". ■

Norbert Tuśnio

MONITORING WIZYJNY W PRZESTRZENI PUBLICZNEJ

We współczesnych miastach czy miasteczkach trudno znaleźć miejsce publiczne pozbawione monitoringu. Kamery obserwują dziś nie tylko ulice, chodniki, sklepy czy osiedla mieszkaniowe. Możemy je spotkać także w parkach, komunikacji miejskiej, na przystankach autobusowych, parkingach, basenach, placach zabaw, przedszkolach, szkołach czy urzędach. Ich obecność nie dziwi dzisiaj nikogo i wydaje się, że stanowi coraz słabszy argument przeciwko aktom wandalizmu, przemocy czy przestępczości. Być może przyczyną takiego stanu był brak regulacji prawnych w zakresie możliwości wykorzystania nagrań jako materiałów dowodowych a także autentyczność tychże materiałów związana z ich „słabą" jakością.

Robert Gabrysiak

Jednakże współczesne technologie rozwiązują problem skutecznej obserwacji i monitoringu przestrzeni publicznej. Przede wszystkim gwarantują one wysoką rozdzielczość obrazu pozwalającą na prawidłowe rozpoznawanie osób czy sytuacji. Początek rewolucji technologicznej w zakresie monitoringu przestrzeni publicznych nastąpił w 2011 roku, kiedy to wdrożono technologię wieloprzetwornikową (multifocal-sensor technologie). Pozwalała ona bowiem na obserwację bardzo dużych obszarów przy zdecydowanie mniejszej liczbie zastosowanych kamer w porównaniu do ilości kamer tradycyjnych PTZ (pan-tilt-zoom). Podczas obserwacji dużych terenów ważne jest aby obraz zapisywać z odpowiednią rozdzielczością, która określona jest w normie DIN_EN 62676-4 i podawana w pix/m (piksel na metr). Norma ta mówi, że dla operatora prowadzącego obserwację „na żywo" parametr ten musi wynosić co najmniej 250pix/m aby mógł on skutecznie rozpoznać osobę.

Tak po krótce wyglądał przełom w rozwoju technologicznym – zapoczątkowany w 2011 r. Aktualnie prognozuje się znaczny wzrost zainteresowania monitoringiem wizyjnym w porównaniu do lat poprzednich – czyli czasów pandemii, która de-facto przyczyniła się do wzrostu zaufania społeczeństwa do nowych technologii w szczególności w zakresie bezpieczeństwa publicznego. Monitoring publiczny może dziś opierać się na takich rozwiązaniach technologicznych jak: sieci 5G, sztuczna inteligencja AI czy sieci „zero trust". Sieć „zero trust" swój szczególny rozkwit przeżyła właśnie w czasie pandemii i stała się właściwą metodą ochrony sieci wewnątrz organizacji. Dziś sieć „zero trust" oznacza, że każde urządzenie IP posiadające dostęp do zasobów jest uznawane jako potencjalne zagrożenie – co w przypadku systemów dozoru wizyjnego oznacza konieczność stosowania sygnowanego oprogramowania oraz przeprowadzania regularnych aktualizacji systemu. Ponadto dane z monitoringu należy szyfrować oraz zabezpieczać tożsamość.

Współczesny monitoring wizyjny stawia też duży nacisk na zabezpieczenie nagrań wideo tak, aby nie można było (w razie przechwycenia) nimi manipulować – bowiem tylko autentyczne nagranie nie może być zakwestionowane. W tym celu nagrania zabezpiecza się już na etapie rejestracji – np. poprzez wprowadzenie cyfrowego podpisu do strumienia wideo w momencie przechwytywania. Takie rozwiązanie pozwala udowodnić, że dany obraz pochodzi z konkretnej kamery i został zarejestrowany w określonym czasie – bez naruszania struktury obrazu.

Kolejną nową technologią zdobywającą rynki światowe jest sieć 5G. Sieć ta charakteryzuje się wysoką przepustowością i niewielkimi opóźnieniami. Te cechy sieci 5G mogą stanowić o szerokim jej wykorzystaniu w ramach monitoringu wizyjnego, gdyż pozwoli to budować systemy o wysokim stopniu bezpieczeństwa. Jeśli do tego dołożymy wykorzystanie sztucznej inteligencji AI, która zoptymalizuje monitoring w zakresie wydajności otrzymamy nowoczesny, stabilny, bezpieczny system monitoringu wizyjnego przestrzeni publicznych.

Podsumowując rozwój technologiczny systemów monitoringu możemy zauważyć, że główny trend polega na tworzeniu hybryd – czyli łączeniu wielu rozwiązań systemowych w celu jak naj-

bardziej bezpiecznego zbierania, przechowywania i analizy danych.

Tworząc system monitoringu wizyjnego wybieramy najlepsze rozwiązanie technologiczne. Jednak cały czas musimy pamiętać o właściwej ochronie danych osobowych – czyli wchodzimy w zakres zagadnień RODO. Przetwarzanie danych osobowych przy monitoringu wizyjnym wiąże się z zapisywaniem, przeglądaniem, udostępnianiem, a nawet usuwaniem nagrań zarejestrowanych zdarzeń i osób. To powoduje, że niezwykle istotne jest kontrolowanie dostępu do tych danych.

Pamiętajmy, że monitoring wizyjny jest formą przetwarzania danych osobowych a zatem podlega przepisom RODO. W szczególności chodzi o dane wizerunkowe oraz indywidulane cechy osób czy choćby numery rejestracyjne pojazdów. Warto także dodać, że monitoring nie powinien obejmować rejestracji dźwięku. Prezes UODO uznał, że byłoby to nadmiarowe przetwarzanie danych. Podstawą dopuszczającą zastosowanie monitoringu w przestrzeni publicznej są konkretne przepisy prawa. W zależności od konkretnej sytuacji, podstawa prawna się zmienia. Kluczowe jest także odpowiednie informowanie osób objętych monitoringiem o tym fakcie. Eksperci od ochrony danych osobowych twierdzą, że sama tablica z grafiką kamery nie jest wystarczającym spełnieniem obowiązku informacyjnego ponieważ osoba, której dane dotyczą, musi mieć świadomość skutków płynących z przetwarzania jej danych w formie monitoringu.

Obserwowanie ludzi wywołuje zawsze pewne wątpliwości. W wyniku niedoinformowania lub niewiedzy obserwowanych pojawia się wśród nich wiele pytań i mitów związanych z prawem do stosowania monitoringu, jego legalnością oraz bezpieczeństwem zarejestrowanych danych. Przykładem może być mit mówiący, że nadzór wizyjny jest zawsze formą przetwarzania danych osobowych. Owszem jest on taką formą lecz nie zawsze – np. przy stosowaniu kamer służących do monitorowania terenu ale nie odzwierciedlających wizerunku (kamery podczerwieni pokazują jedynie sylwetki a nie odzwierciedlają wizerunku). Podobnym mitem jest to, że monitoring wizyjny w zakładzie pracy może posłużyć pracodawcy do rozliczania wyników pracy poszczególnych pracowników. Otóż zgodnie z prawem, pracodawca nie może wykorzystywać monitoringu wizyjnego do nadzoru nad realizacją zadań pracowników. Uregulowane to zostało w zmienionym na przepisy o ochronie danych osobowych *Kodeksie pracy.* Nadzór wizyjny w zakładzie pracy może jedynie służyć do zapewnienia bezpieczeństwa pracownikom, ochrony mienia lub kontroli produkcji i ochrony danych produkcyjnych.

Nieco inaczej przepisy RODO traktują monitoring zamontowany na prywatnych posesjach, w celu ochrony mienia prywatnego. Właściciele takich systemów monitoringu nie muszą martwić się przepisami RODO ponieważ przepisy te nie dotyczą przetwarzania danych w celach osobistych lub domowych. Problem jednak pojawia się wtedy, gdy kamery takiego systemu sięgają poza obszar prywatnych posesji – np. obejmują chodnik czy ulicę. W takim przypadku na skutek nagrania osoby lub identyfikowalnego pojazdu dochodzi do przetwarzania danych osobowych, tyle, że w celach prywatnych. UODO podpowiada, że w takim przypadku należy odpowiednio oznaczyć posesję prywatną i w miarę możliwości nie obserwować sąsiednich prywatnych budynków czy terenu publicznego.

Takich jak powyżej i wiele innych dylematów związanych z ochroną danych osobowych może pojawić się podczas wdrażania systemów monitoringu wizyjnego w przestrzeniach publicznych. Należy wtedy sięgnąć po odpowiednie rozporządzenia i przepisy a w razie wątpliwości wszystkie działania konsultować bądź opiniować w odpowiednimi urzędzie – takimi jak UODO. ■

Robert Gabrysiak

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

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

PRENUMERATA

Dział prenumeraty

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

Zamówienie prenumeraty przyjmujemy

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

Prenumerata

Roczna **60 zł**

Prenumerata dostępna także przez

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

SKLEP INTERNETOWY
www.czasopisma.net

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

Lubię to!

Wejdź na nasz profil i polub nas!

www.facebook.com/**ochronaibezpieczenstwo**

KONTAKT

Wydawca

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

Prezes zarządu: **Katarzyna Polesińska**

Dyrektor wydawnicza

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

Redakcja:

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

Robert Gabrysiak
Redaktor prowadzący

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

Lidia Tuchowska
Redaktor/Marketing i PR

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

Katarzyna Kalata-Kieblesz
Kierownik Działu Reklamy

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

Stała współpraca:
Jerzy Ciszewski, Mateusz Gosk, Sebastian Hładun, Dariusz Knapek, Waldemar Kubik, Krzysztof Łangowski, Paweł Łuszcz, Dobrosław Mąka, Cezary Mecwaldowski, Krzysztof Młudzik, Radosław Monia, Sergiusz Parszowski, Szymon Pergał, Adam Radomyski, Robert Poklek, Janusz Sawicki, Stanisław Sulenta, Jerzy Taczalski, Norbert Tuśnio, Damian Żabicki.

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

Łamanie i opracowanie graficzne: WAŻKA Łukasz Piotrowski

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

PATRONAT HONOROWY

RCB Rządowe Centrum Bezpieczeństwa

KNF KOMISJA NADZORU FINANSOWEGO

Instytut Zachodni

CEPOL

URZĄD TRANSPORTU KOLEJOWEGO

ORGANIZATORZY

WAT

SAFETY PROJECT

17-19 października 2022 r.

Hotel Kuźnia Napoleońska
Paprotnia k. Warszawy

SAFE PLACE CONGRESS 2022

V Ogólnopolski Kongres Naukowo-Techniczny

BEZPIECZEŃSTWO BUDYNKÓW UŻYTECZNOŚCI PUBLICZNEJ I INFRASTRUKTURY KRYTYCZNEJ
TERRORYZM I INNE ZAGROŻENIA

WSPÓŁORGANIZATORZY

POLICJA

ZWIĄZEK BANKÓW POLSKICH

Centrum Ratownictwa

GRUPY DYSKOZYCYJNE

INSTYTUT POLITYKI ENERGETYCZNEJ IM. IGNACEGO ŁUKASIEWICZA

KUL 1918

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU
Zakład Studiów Strategicznych
Wydział Nauk Politycznych i Dziennikarstwa

PTBN

PISA

POLALARM

ARITECH

PARTNERZY MEDIALNI

Difin

SPECIAL OPS

a&S POLSKA

OCHRONA i BEZPIECZEŃSTWO

alarmy.org
Portal branży zabezpieczeń mienia

Militaria.pl

MILMAG

więcej informacji na www.safeplace.edu.pl

Dyskretny urok minimalizmu

Elektroniczna klamka ETB-IM do drzwi wewnętrznych z drewna, stali lub PVC

Komfortowe użytkowanie
Wygodna, zabezpieczona przed przekręceniem, odporna na długotrwałą eksploatację

Skuteczna ochrona
Elastyczne nadawanie i zmiana uprawnień dostępowych

Prosta konserwacja
Łatwa wymiana baterii za pomocą standardowych narzędzi

Intuicyjna obsługa
Obsługa przy pomocy kluczy blueSmart lub kart ID

Wysoka jakość
Zaprojektowana oraz wyprodukowana w Münster, Niemcy

Błyskawiczny montaż
Bez wiercenia, okablowania, bez zarysowań na skrzydle drzwi

bluesmart.winkhaus.com