

NR 6/2019 listopad/grudzień

Ochrona Mienia i Informacji

Cena 16,90 (w tym 8% VAT), nr ind. 381756

8 Wywiad z Prezesem Zarządu
SUMA SOLUTIONS

18 Psychologiczne i techniczne aspekty
stanowiska operatora dozoru wizyjnego
Przygotowanie stanowiska

35 Kompendium wiedzy Security Managera
– część 2

49 Audyt bezpieczeństwa Obiektu
– przebieg i tajna broń analityka:
metodyka

 **VIVOTEK**

LICZENIE LUDZI I POJAZDÓW

Systemy liczenia dużej dokładności 3D i 2D

PANORAMICZNE PROJEKTY

Wysokiej wydajności systemy panoramiczne 180°/360°

ANALITYKI I SYSTEMY LPR/LPC

Wysokiej jakości inteligentny monitoring wideo



Sumo

• SOLUTIONS

• EXPERT

■ CONSULTING

■ NINJA

SUMA.COM.PL

**28 LAT DBAMY O BEZPIECZEŃSTWO
LUDZI I MIENIA.**



- **KONCEPCJE**
- **PROJEKTY**
- **MONTAŻ**
- **KONSERWACJA**
- **SERWIS**

- **SYSTEMY SYGNALIZACJI POŻARU**
- **DŹWIĘKOWE SYSTEMY OSTRZEGAWCZE**
- **STAŁE URZĄDZENIA GAŚNICZE**
- **SYSTEMY ODDYMIANIA**
- **SYSTEMY SYGNALIZACJI WŁAMANIA**
- **SYSTEMY KONTROLI DOSTĘPU**
- **SYSTEMY TELEWIZJI PRZEMYSŁOWEJ**
- **SYSTEMY OKABŁOWANIA STRUKTURALNEGO**
- **INTEGRACJA SYSTEMÓW BEZPIECZEŃSTWA**



RAJ International Sp. z o.o.
ul. Wał Miedzeszyński 552B
03-994 Warszawa
tel. 22 679-92-11
raj-biuro@raj-international.net

www.raj-international.net

AKTUALNOŚCI I INFORMACJE BRANŻOWE

- SCHRACK – relacja z VIII Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego w Jachrance 4
- Projekt BMS – podsumowanie IV edycji w Łochowie 5
- Czujki ruchu WXS – nowości Firmy OPTEX 7

WYWIAD

- Z wizytą w SUMA SOLUTIONS – wywiad z Robertem Stanoszem Prezesem Zarządu Firmy** 8

BEZPIECZEŃSTWO

Systemy przeciwpożarowe

- Techniczne środki zabezpieczenia garaży – detektory w garażach i parkingach podziemnych** 10
– artykuł Krzysztofa Majdaka

ZARZĄDZANIE

Bezpieczeństwo pożarowe

- Zarządzanie bezpieczeństwem pożarowym w obiektach wymagających szczególnej ochrony. Skuteczność systemu sygnalizacji pożaru** 13
– artykuł Krzysztofa Majdaka

Ochrona osób i mienia

- Przygotowanie stanowiska operatora systemu dozoru wizyjnego. Aspekty psychologiczne i techniczne** 18
– artykuł Cezarego Mecwaldowskiego i Roberta Pokleka

Nowoczesna detekcja ruchu

- SLIM LINE – nowe oblicze detekcji ruchu** 26
– artykuł Firmy SATEL

Ochrona przeciwpożarowa

- Dopuszczenie do użytkowania wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia – świadectwo dopuszczenia** 28
– artykuł Ilony Majki z CNBOP-u

Świadomość antyterrorystyczna

- Świadomość „antyterrorystyczna” przedsiębiorców – część 2** 32
– artykuł Grzegorza Cieślaka

Ochrona lotnictwa cywilnego

- Kompendium wiedzy Security Managera: Bezpieczny łańcuch dostaw** 35
– artykuł Macieja Korczaka

Zarządzanie ciągłością działania

- Zarządzanie ciągłością działania – jeden z filarów bezpieczeństwa organizacji** 39
– artykuł Huberta Łabęckiego

Zintegrowane systemy bezpieczeństwa

- MAXPRO CLOUD – usługi hostingowe w chmurze** 42
– artykuł Firmy TAP Systemy Alarmowe

Ochrona tajemnic Firmy przed wewnętrznym wrogiem

- Twój współpracownik – twój wróg** 46
– artykuł Michała Czumy

Ochrona Mienia i osób

- Audyt bezpieczeństwa obiektu – tajna broń analityka: Metodyka** 49
– artykuł Krzysztofa Moszyńskiego

PRAWO

Prawo Pracy

- Umowa o zakazie konkurencji na gruncie prawa pracy** 44
– artykuł Radosława Moni

BIZNES

Modele finansowania dla przedsiębiorstw

- Nowy samochód w Firmie ? Jak go sfinansować ?** 54
– artykuł Grupy Auto – Wimar SKODA

OD WYDAWCY

REKLAMODAWCY

SUMA Solutions	I okładka, 8
RAJ	II okładka
Ochrona i Bezpieczeństwo	9
ELA COMPIL	15
SATEL	17, 26–27
MIWI-URMET	23
SECUREX 2020	25
PARTNER	31
PRENUMERATA	38
TAP	41, 42–43
SECURITECH 2020	53
SKODA Auto-Wimar	54–55
SPYSHOP	III okładka
RTcom	IV okładka



Szanowni Czytelnicy,

rzządzanie Ciągłością Działania może przynieść znaczące korzyści mniejszym firmom umożliwiając im budowanie przewagi nad konkurencją, poprawę (poprzez kompleksowe oddziaływanie na każdej płaszczyźnie) bezpieczeństwa i zarządzania ryzykiem czy ochronę interesów klientów i właścicieli.

W zakresie ochrony biznesu przedstawiono temat dotyczący wielu przedsiębiorców jakim jest – Zdrada pracownicza. Jest to temat dość rzadko poruszany dotyczący wielu firm. Autor przedstawił swoje doświadczenia w zakresie analiz praktycznych m.in. kiedy pracownik zaczyna działać na szkodę firmy i co powoduje, że działa na rzecz konkurencji. Temat bezpieczeństwa obiektów zapoczątkowany w nr. 5 został przedstawiony w zakresie – Audytu bezpieczeństwa obiektu. Autor przedstawił w swoim tekście metodykę audytu oraz wskazał ostrzeżenia, zasadzki i najczęstsze wpadki. Poradził jak się wywiązać z nie-trafionych deklaracji i zbyt wcześnie wyciągniętych wniosków. Przedstawił także przebieg audytu, z czym można się spotkać i na co natknąć. Tak dziś gorący temat jakim jest monitoring wizyjny autorzy przeanalizowali pod kątem – Psychologicznych i technicznych aspektów stanowiska operatora dozoru wizyjnego oraz przygotowania stanowiska. W szczególności m.in. omówili dlaczego obserwacja w systemie dozoru wizyjnego sprawia tak wiele trudności. W związku z zapotrzebowaniem branży w przedstawianiu na łamach naszego periodyka tematyki systemów przeciwpożarowych, rozpoczynamy nowy cykl artykułami omawiającymi – Zarządzanie bezpieczeństwem pożarowym w obiektach wymagających szczególnej ochrony przed pożarem oraz skuteczne systemy sygnalizacji pożarowej. W przedmiotowym artykule autor wskazuje obiekty szczególnie chronione, wymagania jakie stawia się skutecznemu systemowi sygnalizacji pożarowej itp. W osobnym tekście przedstawiono bardzo istotny dla bezpieczeństwa obiektów temat, dotyczący technicznych środków zabezpieczenia garaży i parkingów podziemnych. Autor biorąc pod uwagę realne zagrożenia dla tej wrażliwej infrastruktury omówił w artykule w syntetyczny sposób rozwiązania w zakresie stosowanych różnych koniecznych systemów technicznych i potrzebę ich integracji.

Kontynuując serię artykułów autorstwa grupy specjalistów z Centrum Naukowo – Badawczego Ochrony Przeciwożarowej Państwowego Instytutu Badawczego im. Józefa Tuliszkowskiego poświęconej certyfikacji systemów i urządzeń stosowanych w ochronie przeciwpożarowej przedstawiono artykuł przybliżający temat procesu dopuszczenia do użytkowania pewnej grupy szczególnych wyrobów. Wyrobami tymi są urządzenia przeciwpożarowe, które bez wątpienia mają wpływ na szeroko pojęte bezpieczeństwo pożarowe, przede wszystkim umożliwiając przeprowadzenie skutecznej i bezpiecznej ewakuacji ludzi w sytuacji zagrożenia oraz zwiększając bezpieczeństwo ekip ratowniczych podczas prowadzenia działań ratowniczo-gaśniczych.

Publikujemy także wywiad, artykuły, prezentacje kilku firm, Suma Solutions – wywiad z prezesem zarządu panem R. Stanoszem na temat historii firmy jej aktualnej działalności oraz planów na przyszłość, TAP – wyrobu MAXPRO® Cloud firmy Honey-

Szósty ostatni w tym roku, a także ostatni pod dotychczasowym tytułem, numer naszego dwumiesięcznika poświęcony został tak jak numer piąty, zagadnieniom związanym z ochroną i bezpieczeństwem przedsiębiorców, dla których wysoki poziom ochrony i bezpieczeństwa stanowi gwarancję zachowania wypracowanej pozycji na rynku.

Tak jak na wstępie wspomniałem, w tym wydaniu kontynuujemy cykl artykułów mających swój początek w numerze piątym. I tak poczynawszy od porad prawnych, drugi artykuł z tego cyklu dotyczy tematu, jakim jest umowa o zakazie konkurencji na gruncie prawa pracy. W niniejszej publikacji zostały zaprezentowane w sposób skrótowy najważniejsze informacje dotyczące możliwości wprowadzenia zakazu konkurencji, zarówno w trakcie trwania stosunku pracy, jak i po jego zakończeniu. W tematyce zarządzania ochroną i bezpieczeństwem lotnictwa w kolejnej części Kompendium wiedzy Security Managera zawarto opis tematu dot. bezpiecznego łańcucha dostaw (ładunku tzw. cargo i poczty) w oparciu o obowiązujące przepisy z zakresu ochrony lotnictwa cywilnego. W szczególności przedstawiono m.in. proces obsługi ładunków, proces certyfikacji/wymogi, zagrożenia/wyzwania itp. Kontynuując rozpoczętą w poprzednim numerze tematykę – Świadomości „Antyterrorystycznej” przedsiębiorców – znalazły się informacje dot. działań antyterrorystycznych w polityce bezpieczeństwa – czyli o tym, że procedura nie jest instrukcją, a instrukcją procedurą. Ponadto przedstawiono formy zdarzenia o charakterze terrorystycznym – obszary, w których priorytety mogą być ze sobą sprzeczne. W obszarze tak istotnym dla działalności wielu firm jakim jest Zarządzanie Ciągłością Działania jako jednego z filarów bezpieczeństwa organizacji, autor przedstawił temat zarządzania Ciągłością Działania jako propozycję dla dużych korporacji czy sektora publicznego (infrastruktury krytycznej, operatorów usług kluczowych). Omówił mi.in zasady zarządzania Ciągłością Działania, które mają zastosowanie dla wszystkich organizacji, bez względu na wielkość czy profil prowadzonej działalności. Wykazał, że w rzeczywistości sprawne Za-

well w pełni zintegrowanej platformy umożliwiającą podłączenie do chmury systemów sygnalizacji włamania i napadu, kontroli dostępu oraz telewizji dozorowej lub kombinacji tych systemów, Satel – nowej serii czujek ruchu SLIM LIN, urządzeń, które oprócz wysokiej skuteczności w wykrywaniu ruchu w chronionym obszarze, oferują szereg dodatkowych, rozwiązań, Skoda – Grupy Auto Wimar – nowych sposobów finansowania zakupu samochodów, które powinien znać każdy przedsiębiorca, outsourcingowych modeli finansowania.

Ponadto tak jak w poprzednich numerach publikujemy relacje z odbytych bieżących wydarzeń branżowych, którymi były VIII edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy oraz Konferencja Projekt BMS 2019.

Miło mi również poinformować, że dwumiesięcznik „Ochrona Mienia i Informacji”, po przejściu ewolucji tematyki wynikającej z aktualnych potrzeb branży, od początku 2020 roku będzie się ukazywał pod nowym logo i tytułem „Ochrona i Bezpieczeństwo obiektów i biznesu”. Zapewniam, że periodyk w dalszym ciągu będzie pełnił rolę doradczą, informacyjną, propagującą wiedzę w obszarze ochrony i bezpieczeństwa obiektów oraz biznesu. Cykle artykułów mające swój początek w aktualnym tytule oczywiście będą kontynuowane. Dbając o wysoką jakość przedstawianych treści, w szczególności, w nowym tytule będą publikowane artykuły autorstwa wysokiej klasy praktyków, ekspertów i naukowców z zakresu organizacji, zarządzania, prawa, zapewnienia ciągłości działania, efektywnego wykorzystywania nowych technologii, tworzenia planów i procedur ochrony oraz bezpieczeństwa, projektowania oraz instalacji systemów, upowszechniania świadomości aktualnych zagrożeń. Czasopismo skupi się

także na propagowaniu praktycznej wiedzy z zakresu zarządzania bezpieczeństwem i ochroną, wykorzystywania nowoczesnych urządzeń i technologii, optymalnego projektowania, instalacji i eksploatacji systemów oraz urządzeń służących do wykrywania oraz sygnalizacji zagrożeń takich jak np. materiałów i urządzeń wybuchowych, pożarów, napadów i włamań, aktów bezprawnej ingerencji, kontroli dostępu, monitoringu wizyjnego, systemów łączności, systemów ochrony terenu i infrastruktury itp. W nowym tytule czytelnicy znajdą prezentacje wybranych zagadnień dotyczących terroryzmu, cyberbezpieczeństwa, bezpieczeństwa danych osobowych, ochrony informacji niejawnych i wrażliwych, ratownictwa, ochrony przeciwpożarowej, ochrony infrastruktury krytycznej i obiektów specjalnych, ochrony i bezpieczeństwa lotnictwa cywilnego, ochrony i bezpieczeństwa publicznego oraz osobowego, szeroko rozumianego bezpieczeństwa biznesu itp. Na łamach „Ochrony i Bezpieczeństwa” będzie można również znaleźć informacje na temat wydarzeń z życia branży ochrony i bezpieczeństwa w tym w szczególności: wystaw partnerów technicznych i konferencji naukowych, których nasze wydawnictwo będzie współorganizatorem i partnerem medialnym.

Korzystając z okazji, że jest to ostatnie wydanie naszego periodyka w tym roku, chciałbym wraz z całym zespołem redakcyjnym życzyć naszym Czytelnikom owocnej i przyjemnej lektury, Zdrowych i Wesołych Świąt Bożego Narodzenia oraz Szczęśliwego Nowego 2020 roku.

Robert Mościcki
Redaktor Naczelny



*Z okazji Świąt Bożego Narodzenia
i zbliżającego się Nowego 2020 Roku
wszystkim naszym Czytelnikom i Partnerom
najlepsze, świąteczno – noworoczne życzenia
składa Redakcja.*

23–24 PAŹDZIERNIKA 2019 R. VIII EDYCJA OGÓLNOPOLSKICH DNI ZINTEGROWANYCH SYSTEMÓW BEZPIECZEŃSTWA POŻAROWEGO – SCHRACK SECONET I PARTNERZY PODSUMOWANIE

W dniach 23–24 października 2019 roku, w Hotelu Windsor w Jachrance, odbyła się już VIII edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy. W ciągu dwóch dni na wydarzenie zarejestrowało się łącznie ponad 570 osób! Organizatorzy również w tym roku umożliwili udział w wydarzeniu tym, którzy nie mogli osobiście pojawić się na miejscu – przez dwa dni była prowadzona transmisja LIVE w Internecie.

Ogromne zainteresowanie wydarzeniem potwierdza sensowność, a nawet konieczność, organizacji częstszych spotkań merytorycznych w branży systemów bezpieczeństwa. Schrack Seconet Polska, wychodząc naprzeciw oczekiwaniom rynku, każdego roku przygotowuje wiele nowości – dotyczą one zarówno samej organizacji wydarzenia, sposobów komunikacji z uczestnikami (różnorodne formy przekazu), ale przede wszystkim coraz głębszej, dokładniejszej analizy problemów pojawiających się w trakcie projektowania i realizacji obiektów różnego przeznaczenia.

Podczas dwóch dni wykładów merytorycznych, paneli dyskusyjnych oraz pokazów zadziałania urządzeń uczestnicy wydarzenia zapoznali się z aktualnymi zmianami prawnymi, wytycznymi, normami i najlepszymi praktykami w zakresie procesów oceny zagrożeń, tworzenia koncepcji, projektowania, realizacji i eksploatacji zintegrowanych systemów bezpieczeństwa pożarowego, technicznego i fizycznego. Studia przypadków oparte na pokazach zadziałania urządzeń były na bieżąco komentowane przez specjalistów branżowych. Praktyki i możliwości zastosowania najnowszych rozwiązań technicznych proponowane przez firmy partnerskie oceniali uznani na rynku eksperci. Podczas tej edycji



wydarzenia po raz pierwszy podjęto próbę sformułowania standardu oceny jakości wdrożenia zintegrowanego systemu bezpieczeństwa ze szczególnym naciskiem na ocenę skuteczności stosowanych technologii i rozwiązań organizacyjnych i ich wpływu na skuteczność bezpiecznej ewakuacji osób z obiektów budowlanych różnego przeznaczenia.

Nowością tegorocznego wydarzenia były dodatkowe sale warsztatowe, w których swoje prezentacje i zajęcia poprowadzili **eksperti ds. pożarowych oraz specjaliści od zarządzania ryzykiem** – na co dzień oceniający zagrożenia i stan przygotowania budynków do minimalizacji skutków zdarzeń kryzysowych **z ramienia firm ubezpieczeniowych**. Podczas tych warsztatów poruszane kwestie obejmowały zagadnienia dotyczące odstępstw, ana-





lizi przypadków wykraczających poza ramy wytycznych i prawne oraz ocenę skutków zdarzeń kryzysowych z punktu widzenia warunków wypłaty lub wstrzymania odszkodowania za straty. W tym roku warsztaty odbywały się równolegle w **13 salach!**

Organizatorzy zaskoczyli uczestników jeszcze jedną zmianą formuły: zajęcia warsztatowe, kończące obydwie dni wydarzenia, miały charakter sesji pytań i odpowiedzi oraz wymiany poglądów. Były to otwarte panele dyskusyjne, podczas których specjaliści z różnych dziedzin mieli jeszcze więcej możliwości uzyskania odpowiedzi na nurtujące ich kwestie z zakresu prawa, techniki oraz praktyki wykonawczej i użytkowania systemów bezpieczeństwa w obiektach komercyjnych, przemysłowych, użyteczności publicznej, muzeach itp.

W wydarzeniu wzięli udział producenci najważniejszych stosowanych w obiektach budowlanych urządzeń i systemów bezpieczeństwa, takich jak: SSP, DSO, SUG, BMS, SMS, CCTV (VSS), SKD, DCIM, interkomowych i powiadamiania o zagrożeniach, systemu integrującego urządzenia przeciwpożarowe (SIUP), przyzywowych i komunikacji, kontroli rozprzestrzeniania się dymu i ciepła, sterujących oddzieleniami pożarowymi i innymi instalacjami technicznymi obiektu.



Udział w dwudniowych warsztatach zostanie potwierdzony wspólnym zaświadczeniem, wystawionym przez Schrack Seconet Polska oraz Partnerów spotkania. **Otrzymanie dokumentu z kompletem podpisów wszystkich producentów uzależnione jest od udziału uczestnika w poszczególnych sesjach szkolenia.**

Schrack Seconet Polska w imieniu swoim oraz wszystkich tegorocznych Partnerów projektu, składa serdeczne podziękowania wszystkim prelegentom, uczestnikom, przedstawicielom instytucji oraz uczelni technicznych, patronom merytorycznym i medialnym. Organizatorzy dziękują także wszystkim Partnerom projektu za wspólną, wielotygodniową pracę nad całokształtem szkolenia.

Firma Schrack Seconet Polska zaprasza do udziału w kolejnej edycji Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2020. **Termin IX edycji zostanie ogłoszony już w grudniu 2019 roku!**

Osoba do kontaktu:

Marta Nowak – Dyrektor Marketingu marta.nowak@schrack-seconet.pl

PROJEKT BMS 2019: PODSUMOWANIE CZWARTEJ EDYCJI

6–7 listopada 2019 w Folwarku Łochów konferencja Projekt BMS zgromadziła po raz kolejny przedstawicieli branży nieruchomości oraz inteligentnych rozwiązań budynkowych. Czwarta edycja była wyjątkowa pod wieloma względami. Przede wszystkim z uwagi na szerokie grono ekspertów i partnerów, którzy przedstawili najbardziej aktualne tematy i trendy rządzące rynkiem. Uwagę zwracała także aktywność i zaangażowanie uczestników w rozmowy o istotnych problemach cyberbezpieczeństwa, technologii Cloud Computing i Big Data czy multimediów w inteligentnych budynkach.

Szczególne miejsce w programie Projekt BMS 2019 zajął panel dyskusyjny moderowany przez **Bartosza Dobrowolskiego**, założyciela PropTech Poland oraz członka zarządu RICS Polska. O tym czy:

- *PropTech to cyrk innowacji czy faktyczna szansa na przewagę konkurencyjną?*





- *Jakie realne zmiany można wprowadzić w zarządzaniu nieruchomościami dzięki technologii?*
- *Jakie technologie sprawdzają się w sektorze nieruchomości?*
- *Jak rozwiązania PropTech integrują się z systemami BMS?*
- *Czy można „wkomponować” nowe technologie w stare budynki?*
- dyskutowali **Maciej Wiśniewski**, Prezesa Zarządu IFMA Polska; **Szymon Konop**, Business Development Manager, Hilo Solutions sp. z o.o.; **Krzysztof Swaczyński**, Wiceprezes i założyciel Seqred S.A.; **Krzysztof Mazur** – Prezes Zarządu i współzałożyciel General Automatic oraz **Karol Kłos**, Prezes Zarządu, Centrum Informacji Branżowej Sp. z o.o.

Nowością czwartej edycji Projekt BMS były specjalnie przygotowane przez firmę WAGO warsztaty: *Rozwiązania „chmurowe” do zastosowań w automatyce budynkowej. Od kompleksowego, zaawansowanego BMS po prosty monitoring.* Spotkanie spotka-

ło się z ogromnym zainteresowaniem, które zapewne zaowocuje kolejnymi edycjami.

Partnerami wydarzenia były firmy: APA Group, Finder, WAGO, ATEN, Bitner, Distech Controls, Eltcrac System, GEZE, Miwi Urmet, Produal, Roger, SAMSUNG, Veracomp, Beckhoff, Bin-e, Connectorio, Contemporary Controls, Synergy Team Polska, Smart in, SMAY.

Wsparcie merytoryczne zapewnili: Proptech Poland, IFMA Polska, PLGBC Polskie Stowarzyszenie Budownictwa Ekologicznego, Polska Rada Facility Management, Seqred, SSW Pragmatic Solution, General Automatic, Hilo Solution.

Strona konferencji: www.projektbms.pl

Galeria zdjęć: <https://bit.ly/2NR4IAI>

Kontakt:

Uczestnicy: Łukasz Haliniak | +48 603 302 747 | lhliniak@lockus.pl

Partnerzy: Ewa Owsiak, T: 603 748 838, eowskiak@lockus.pl

Małgorzata Mogilska, T: 605 868 610, mmogilska@lockus.pl



DETEKCJA ZEWNĘTRZNA, NA KTÓREJ MOŻESZ POLEGAĆ

Znana z niezawodnych produktów firma OPTEX rozszerzyła swoją ofertę o panoramiczne, zewnętrzne czujki ruchu o szerokim kącie detekcji 180 stopni – WXS. Urządzenia z tej serii pozwolą na jeszcze bardziej skuteczną ochronę obszernych terenów.



W skład serii WXS wchodzi zarówno czujki PIR jak i PIR+MW wyróżniające się szerokim kątem zasięgu detekcji – 180 stopni. Urządzenia idealnie sprawdzają się w ochronie rozległych terenów przed domem czy też dachów większych budynków. W takich sytuacjach instalatorzy najczęściej wykorzystywali dwie czujki zwrócone tyłem do siebie, co nie było jednak rozwiązaniem idealnym.

Funkcjonalność jednej czujki WXS odpowiednia dwóm standardowym czujkom o kącie detekcji poniżej 90 stopni. Przewagą czujki WXS jest również możliwość niezależnego ustawienia obszaru i czułości detekcji, zarówno dla lewej, jak i dla prawej strony. Ulepszona funkcja antymaskingu sprawia, że czujka działa stabilniej, nie reagując na silne nasłonecznienie, krople wody spływające po soczewce czy też małe owady, które się na niej znalazły.

Dodatkowe modele dualne (PIR+MW) wykazują stabilne działanie nawet przy zastosowaniu w trudnych warunkach, gdzie występują silne zakłócenia świetlne. Czujkę można wieszać na dwóch wysokościach 0,8–1,2 m i 2 m. Wszystko to razem sprawia, że czujki serii WXS wyjątkowo wszechstronne i można je z łatwością dopasować do wymagań różnych aplikacji.

 **OPTEX**
www.optex.com.pl

Reklama

PIONIERSKIE WYDANIE NA POLSKIM RYNKU



Katalog produktów i rozwiązań przeznaczonych
dla osób starszych i niepełnosprawnych

Zainteresuje z pewnością też ich opiekunów
oraz wszystkich, którzy zajmują się projektowaniem
i adaptacjami mieszkań na potrzeby osób starszych
i niepełnosprawnych (architektów i projektantów
branżowych)

MARKETING

Justyna Górnowicz
j.gornowicz@swiat-szkla.pl, tel.: 602 786 268

REDAKCJA

Krzysztof Zieliński
k.zielinski@swiat-szkla.pl, tel.: 605 890 789

Wojciech Kołodziejski
w.kolodziejski@swiat-szkla.pl, tel.: 22 53 53 062

Opracowany przez
redakcję miesięcznika
Świat Szkła
w ramach Kampanii
Dom Komfortowy



Z REDAKCYJNĄ WIZYTĄ W FIRMIE SUMA SOLUTIONS

– ROZMOWA Z PREZESEM ZARZĄDU
PANEM ROBERTEM STANOSZEM



OMil: Suma Solutions jest firmą, która od wielu lat funkcjonuje na polskim rynku. Czy mógłby Pan przybliżyć czytelnikom historię powstania firmy i jej rozwoju?

RS: Tak, nasza firma funkcjonuje od 30 lat. Jesteśmy rodzinną firmą, założoną przez mojego ojca razem z dziadkiem. Przez te lata parę razy zmienialiśmy sposób działania firmy ale zawsze poruszaliśmy się w obszarze ochrony, zaczynaliśmy od handlu bronią, usług ochrony aż do ostatnich osiemnastu lat, gdzie skupiamy się na technicznych środkach ochrony mienia.

OMil: Firma znana jest z różnego rodzaju systemów bezpieczeństwa, czy mógłby Pan wymienić jakiego rodzaju systemy są oferowane w Suma Solutions.

RS: Naszą specjalizacją są sieciowe systemy wideo monitoringu. Nasze działania skupiają się na rynkach wertykalnych i tam upatrujemy szans na biznes. Prowadzimy również dystrybucję produktów ale kształtujemy ją w kierunku dystrybucji w wartości dodatkowe. Razem z naszymi Partnerami od wielu lat działamy w branży kolejowej, bezpieczeństwie publicznym oraz mocno rozwijamy obszar działań w segmencie Smart City.

OMil: Jak wygląda współpraca ze zlecającymi? Wiadomo, że ze względu na specyfikę obiektów, każdy z kontrahentów może mieć inne wymagania.

RS: Naszym priorytetem jest bliska współpraca z naszymi Partnerami i inwestorami, z którymi planujemy wspólne działania i sukcesywnie ją wdrażamy. Wprowadziliśmy wiele narzędzi wspierających naszych partnerów i inwestorów w pracy z inwestycją. Naszym celem jest zaoferowanie inwestorowi pakietu korzyści, synergii całego kanału od sprzedaży przez integrację do eksploatacji. W tym kierunku będziemy rozwijać firmę.



OMil: Z jakimi producentami systemów bezpieczeństwa firma współpracuje?

RS: Prowadzimy dystrybucję produktów takich producentów jak VIVOTEK, Milestone Systems, Sony, Bosch czy Senstar. Nie mamy rozwiązań dla każdego klienta ale nasi Partnerzy uzupełniają naszą ofertę, swoją ofertą w pracy z inwestorem. To przy pomocy tych rozwiązań partnerskich pomagamy poprawiać bezpieczeństwo różnych obiektów. Nie zamykamy się na inne rozwiązania, które z powodzeniem wdrażamy u klientów. Dysponujemy też paroma autorskimi rozwiązaniami opracowanymi przez naszych partnerów, które oferujemy tylko w sprzedaży zamkniętej.

OMil: Poza sprzedażą i dystrybucją systemów, specjalizujecie się Państwo w szkoleniach i serwisie B2B. Czemu w głównej mierze poświęcone są organizowane przez Firmę szkolenia?

RS: Staramy się aby nasze szkolenia dotyczyły rozwiązań innowacyjnych, dających Partnerowi nowe możliwości, może nową perspektywę/spojrzenie na zagadnienie czy określoną problematykę. Chcemy

aby oprócz samego głównego trendu rynkowego podążania w rywalizacji cenowej pokazać Partnerom innowacyjne sposoby ochrony technicznej obiektów. W roku 2020 nasz program szkoleniowy będzie rozbudowany o dodatkowe elementy wspierające Partnerów. W roku 2020 skupimy się na ułatwieniu kontaktu i użytkowaniu synergii we wspólnym działaniu inwestora z ekspertami branżowymi.

OMil: W jakich lokalizacjach (obiektach) znajdują zastosowanie Państwa rozwiązania. Czy mógłby Pan wymienić kilka sztandarowych realizacji firmy?

RS: Nasze rozwiązania można bez trudu zobaczyć w branży kolejowej, w wielu nowych pociągach, na przejazdach kolejowych, w systemach ITS-owych i miejskich monitoringach np. ITS w Warszawie, na powierzchniach handlowych np. wdrożenie systemu liczącego ludzi we Wrocław Fashion Outlet (150 kamer liczących 3D) lub system liczący samochody w galerii Kazimierz Kraków. Mamy bardzo dużo wspólnych sukcesów z naszymi Partnerami. Wspólne wdrożenia prezentujemy na naszych szkoleniach. Zachęcamy firmy poszukujące partnerów biznesowych do kontaktu.

OMil: Jak wyglądają Państwa plany na najbliższe lata?

RS: Głównym naszym celem jest rozwój naszej sieci Partnerskiej, której usługi oferujemy inwestorom. Inwestorzy zyskują sprawdzonych Partnerów, Partnerzy wdrożenia, my zaś sprzedaż produktów. W roku 2020 będziemy rozwijać sieć naszych ekspertów poprzez nowe programy szkoleniowe i oferować ich usługi inwestorom.

OMil: Pozostaje nam zatem życzyć powodzenia i dalszego rozwoju, dziękuję za rozmowę Lidia Tuchowska.

Od wydania nr 1/2020

**Ochrona
Mienia
i Informacji**

zmienia nazwę i logo na



**OCHRONA
i BEZPIECZENSTWO**
OBIEKTÓW I BIZNESU



TECHNICZNE ŚRODKI ZABEZPIECZENIA GARAŻY – DETEKTORY W GARAŻACH I PARKINGACH PODZIEMNYCH

Zagrożenia, z którymi możemy spotkać się w garażach

Obecnie, jednymi z coraz liczniej powstających obiektów budowlanych są wielopoziomowe garaże podziemne i parkingi nadziemne (nazemne) lokowane najczęściej przy centrach handlowych, w obrębie wielorodzinnych budynków mieszkalnych lub funkcjonujące w systemie Park & Ride (P+R) – „Parkuj i Jedź”. W zamkniętej lub częściowo otwartej przestrzeni parkingowej, gdzie jednocześnie może być skupiona duża liczba pojazdów silnikowych, występuje zwiększone ryzyko pożarowe. Gwałtowne rozprzestrzenianie się ognia prowadzi do znacznych strat materialnych oraz utrudnia ewakuację osób zagrożonych. W przypadku parkingów jako obszarów otwartych lub fragmentarycznie wydzielonych osłonami, trudno sięgnąć po jakiegokolwiek urządzenia detekcyjne bądź ograniczające rozprzestrze-

nianie się pożaru, co w dużej mierze związane jest z oddziaływaniem warunków atmosferycznych. W przypadku obiektów zamkniętych, wydzielonych przegrodami budowlanymi, należy wdrożyć sprawdzone, specjalne rozwiązania techniczne. Są bardzo skuteczne, a jednocześnie łatwe do zaprojektowania i wykonania. Strefy garażowe, gdzie nierzadko składowane są też opony, materiały pędne, oleje i inne płyny eksploatacyjne, charakteryzują się dużą gęstością obciążenia ogniowego. Przyczynia się do tego gremialne łamanie warunków eksploatacji garaży, które zostały określone w przepisach techniczno-budowlanych i przeciwpożarowych oraz konkretnych regulaminach użytkowania. Popularność atrakcyjnego z uwagi na cenę paliwa silnikowego LPG powoduje, że parkingi zapełniają się autami z podwójnym układem zasilania. Rozszczelnienie wadliwej instalacji gazowej LPG w pojeździe stanowi poważne

ryzyko wybuchu, którego skutkiem może być pożar, a nawet katastrofa budowlana. Innym zagrożeniem, które upowszechniło się w ostatnich latach jest możliwy zapłon czynnika chłodniczego pochodzenia chemicznego HFO-1234yf, stosowanego w systemach klimatyzacji nowych modeli samochodów. Jego efektem ubocznym jest też wydzielanie się silnie trującego fluorowodoru. Warto zauważyć, że nawet w ogólnodostępnych garażach miejsce zajmują luksusowe i kosztowne pojazdy. Chcąc zabezpieczyć je przed zniszczeniem, uszkodzeniem lub utratą, oprócz ryzyka pożarowego, należy wziąć pod uwagę możliwość dokonania kradzieży, aktów wandalizmu lub wystąpienia innych nadzwyczajnych zagrożeń. Dlatego konieczne jest zastosowanie wielu różnych systemów detekcyjnych i alarmowych.

Systemy detekcji zagrożeń do zabezpieczenia garaży

Głównym punktem analizy potencjalnych zagrożeń w odniesieniu do omawianych obiektów jest ryzyko zapłonu, a w konsekwencji rozwój pożaru. Do ograniczania jego skutków wykorzystuje się system zamknięć przeciwpożarowych – bram i grodzi wyodrębniających wybrane pomieszczenia i strefy. Powszechnie stosowane są również systemy wentylacji pożarowej. Istotnym problemem występującym w trakcie akcji gaśniczych prowadzonych w garażach jest silne zadymienie, które utrudnia ratownikom lokalizację ogniska pożaru. Spalaniu, któremu ulegają łatwopalne elementy wyposażenia wnętrza samochodów oraz ogumienie, towarzyszy wydzielanie się dużej ilości gęstego, czarnego dymu. W takich warunkach, widoczność w zamkniętej bryle garażu jest praktycznie zerowa. Pożar może być spowodowany też umyślnie jako akt wandalizmu, terroru lub czyn służący zatarciu śladów przestępstw albo innych czynności



prawnie zabronionych. Na rynku dostępne są systemy bezpieczeństwa służące do identyfikacji i zwalczania różnorodnych zagrożeń. Do systemów detekcyjnych wykorzystywanych w garażach i parkingach podziemnych należą:

Systemy Sygnalizacji Pożaru (SSP)

– najczęściej bazujący na optycznych, punktowych czujkach dymu, z możliwością ręcznego uruchamiania za pomocą przycisków alarmowych ROP. Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. z 2010 Nr 109 poz. 719 z późn. zm.) *stosowanie SSP jest wymagane w garażach podziemnych, w których strefa pożarowa przekracza 1 500 m² lub obejmujących więcej niż jedną kondygnację podziemną*. W praktyce system ten spotkamy dużo częściej.

Detektory gazów – najczęściej stosowane są detektory gazów wybuchowych lub toksycznych, tlenu a także związków z grupy chloro- i fluoropochodnych węglowodorów alifatycznych tzw. Freonów.

Obowiązek stosowania systemów detekcji tlenu węgla (CO) i propan-butanu (LPG) w garażach podziemnych wynika z treści rozporządzenia w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. Nr 75, poz. 690 z późn. zm.). Zgodnie z § 108 ww. rozporządzenia w *garażu zamkniętym w przypadku gdy wymagane jest stosowanie wentylacji mechanicznej, musi być ona sterowana czujkami tlenu węgla lub gazu propan-butan, jeśli dopuszcza się w nim parkowanie samochodów zasilanych gazem propan-butan i poziom podłogi znajduje się poniżej poziomu terenu*. Detektory gazów wybuchowych należą do grupy urządzeń przeciwpożarowych, zabezpieczają przestrzeń przed powstaniem wybuchu i ograniczają jego skutki, a zatem wpływają na ryzyko rozwoju pożaru.



Fot. 1. Przykład tablicy informującej o wyposażeniu obiektu w monitoring wizyjny

System Sygnalizacji Włamania i Napadu (SSWiN)

zabezpiecza obiekt przed wtargnięciem na jego teren osób niepowołanych w celu dokonania kradzieży, dewastacji lub działań powiązanych. Oprócz funkcji detekcyjnej i alarmowej może realizować też zadania sterownicze. Systemy SSWiN występują zarówno w technologii przewodowej jak i bezprzewodowej oraz umożliwiają mobilną kontrolę np. przy pomocy telefonu komórkowego. Do ich elementów składowych należą czujki, centrale alarmowe, manipulatory oraz urządzenia wyjściowe tj. sygnalizatory, urządzenia monitoringu i powiadamiania (GSM, telefon, radio, e-mail), urządzenia wykonawcze, w tym rejestrujące sytuację alarmową. Czujki dostarczają informacje o naruszeniu strefy bezpieczeństwa, wystąpieniu sytuacji alarmowej lub przekroczeniu wartości zadanej wybranego parametru. Do najczęściej stosowanych rodzajów czujek należą:

- czujki ruchu, głównie pasywne podczerwieni (PIR), mikrofalowe (MW) oraz ultradźwiękowe (US) oraz dualne wykorzystujące jednocześnie te dwa detektory;
- czujki otwarcia drzwi, okien, najczęściej magnetyczne, zwane też kontaktowymi lub czujki elektromechaniczne stykowe;
- czujki aktywne złożone z nadajnika i odbiornika, które reagują na przerwanie wiązki między nadajnikiem, a odbiornikiem;
- czujka stłuczenia szyby, mikrofonowe urządzenie reagujące na częstotliwości fal charakterystyczne dla uderze-

nia w tafłę szklaną oraz dla tłuczenia szkła;

- czujki udarowe (wibracyjne) reagujące na wstrząsy będące następstwem uderzenia;
- czujki przekroczenia progowego poziomu cieczy i inne.

W garażu lub na parkingu, ze względu na specyfikę chronionych przestrzeni i pomieszczeń, w ramach SSWiN najlepiej sprawdzają się dualne czujki ruchu PIR+MW, zarówno modele z optyką szerokokątną, jak i kurtynowe. Jako elementy ochrony obwodowej stosowane są czujki magnetyczne, w tym najazdowe instalowane przy bramach. System SSWiN może być zintegrowany z innymi instalacjami zamontowanymi w budynku (np. monitoringu wizyjnego, sygnalizacji pożarowej, kontroli dostępu), co pozwala na wygodne i efektywne zarządzanie bezpieczeństwem obiektu.

System Telewizji Przemysłowej (CCTV)

tzw. monitoring wizyjny CCTV opiera się na obserwacji, rejestrowaniu i archiwizacji obrazu. Rozwiązanie to jest bardzo rozpowszechnione w obiektach użyteczności publicznej, ale sprawdza się również w zastosowaniach osób prywatnych. Telewizja przemysłowa składa się z kamer rejestrujących obraz i rejestratorów, które go utrwalają zapisując na nośnikach pamięci, a także monitorów umożliwiających bieżącą obserwację i ułatwiających sterowanie kamerami ruchomymi. Obecnie w związku z nowymi przepisami unijnymi (RODO) o stosowaniu systemów monitoringu i rejestracji wideo w obiekcie informują stosowne oznaczenia. Przykład takiej informacji pokazano poniżej.

Każdy z wyżej przedstawionych detektorów przewidziany został do wykrywania określonego zagrożenia. Poniżej przedstawiono przykłady zastosowania detektorów odpowiednich do wykrywania typowych zdarzeń alarmowych w garażach podziemnych. Najlepszy efekt uzyskuje się poprzez kompilację tych rozwiązań,



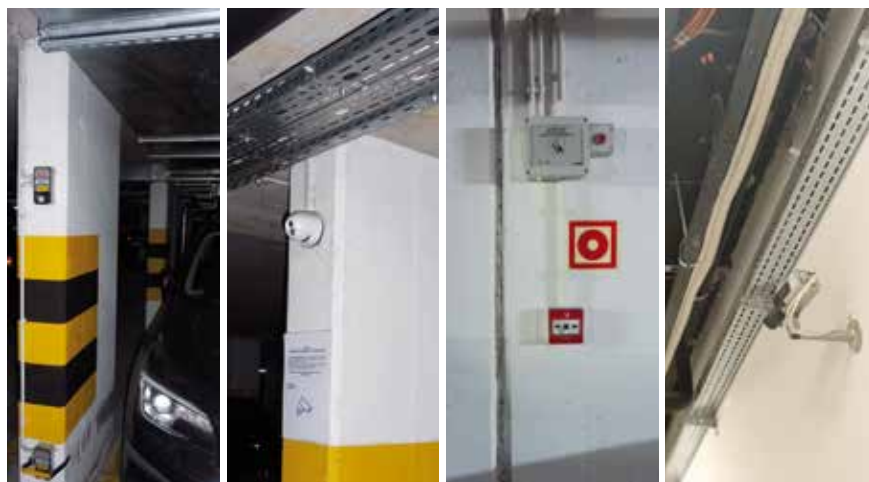
Rys. 1. Detektory zagrożeń stosowane w garażach

tak aby poszczególne systemy mogły się wzajemnie przenikać i uzupełniać.

O doborze zabezpieczeń decyduje inwestor, zarządca lub właściciel stosownie do potrzeb i możliwości. Poniżej przykład typowych zabezpieczeń spotykanych w większości garaży wielostanowiskowych. Wśród nich są pożarowe czujki dymu i ręczne ostrzegacze pożarowe, detektory gazów wybuchowych, kamery stałe i obrotowe, czujki ruchu oraz stosowane w drzwiach i bramach czujki magnetyczne tzw. kontaktrony.

Podsumowanie

Hale garażowe wielostanowiskowe to przestrzenie, w których występuje wysoki poziom wielu zagrożeń. Są to najczęściej przestrzenie ogólnodostępne lub takie, których użytkownikami jest duża liczba osób wpływa na ryzyko wystąpienia zagrożeń. Prowadzenie działań gaśniczych w tego typu obiektach jest zawsze utrudnione. Wysoka temperatura, silne zadymienie i wydzielanie się trujących gazów ograniczają możliwość szybkiego opanowania pożaru. Parametry miejsc postojowych, a przede wszystkim niewielka odległość pomiędzy autami, wpływają na błyskawiczne rozprzestrzenianie się ognia i powodowanie znacznych strat materialnych w związku z doszczętnym zniszczeniem pojazdów i naruszeniem infrastruktury budynkowej. Katalog zagrożeń związanych z funkcjonowaniem garaży obejmuje też akty terroru, kradzieże i dewastacje. Brak personelu stale obecnego w hali garażowej powoduje, że skuteczną ochronę mogą zapewnić wyłącznie instalacje techniczne oraz systemy automatyki budynkowej. Skuteczność rozwiązań technicznych można zwiększyć poprzez integrację kilku systemów bezpieczeństwa. Bardzo efektywnym rozwiązaniem, w przypadku dostęp-



Fot. 2. Przykład elementów technicznego zabezpieczenia hali garażowej

ności gęstej siatki kamer monitoringu, jest zintegrowanie systemów CCTV i SSP, które polega na automatycznym przełączaniu widoku z kamer rejestrujących obraz z miejsca pożaru, który zdążył wykryć SSP. Pozwala to na błyskawiczną lokalizację miejsca zdarzenia i obiektywną ocenę zagrożenia. W obecnych czasach integracja systemów bezpieczeństwa rozwijanych przez różnych producentów nie stanowi już większego problemu. Niegdyś systemy CCTV i SSWiN najczęściej konfigurowano jako niezależne, obecnie już od początku eksploatacji są integrowane i niekiedy zespalone z systemem przeciwpożarowym. Przykładowo, w momencie wykrycia ruchu lub innego zjawiska sta-

nowiącego kryterium alarmu dla czujek systemu SSWiN, następuje automatyczne uaktywnienie CCTV w strefie alarmowej i rejestracja obrazu ze zdarzenia. Wykrycie zjawiska alarmowego zarówno w strukturze SSWiN, jak i w CCTV – każdorazowo generuje alarm. Zapis obrazu zarejestrowanego przez kamery monitoringu stanowi klarowny i niepodważalny dokument o przyczynach wszczęcia alarmu. Kluczem pozostaje jednak zapewnienie ścisłej integracji przy zachowaniu autonomiczności w działaniu na wypadek uszkodzenia poszczególnych systemów, które nie powinno zakłócać pracy pozostałych.

st. kpt. mgr inż. Krzysztof Majdak

Absolwent Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej w Warszawie oraz podyplomowych studiów Politechniki Warszawskiej w zakresie bezpieczeństwa i higieny pracy. Od początku swojej drogi zawodowej związany z Państwową Strażą Pożarną. Doświadczenie zdobywał w pionie kontrolno – rozpoznawczym ukierunkowanym na rozpoznawanie zagrożeń pożarowych w obiektach, a także w pionie operacyjnym, będąc odpowiedzialnym za kierowanie działaniami ratowniczo-gaśniczymi. Przez kilka lat wykonywał obowiązki na stanowisku związanym z ochroną przeciwpożarową obiektów handlowych, a obecnie specjalizuje się w zarządzaniu bezpieczeństwem pożarowym w budynkach muzealnych. Jednym z jego osobistych zainteresowań jest ochrona dóbr kultury na wypadek szczególnych zagrożeń, które łączy z pracą zawodową."

GARAŻ I PARKING PODZIEMNY A SSWiN

W garażu lub na parkingu, ze względu na specyfikę chronionych przestrzeni i pomieszczeń, w ramach SSWiN najlepiej sprawdzą się dualne czujki ruchu PIR+MW. Zarówno modele z optyką szerokokątną, jak i kurtynowe. Zastosowanie znajdą także czujki magnetyczne, w tym najazdowe, instalowane przy bramach. System alarmowy można integrować z innymi instalacjami obecnymi w obiekcie (np. detekcji gazów, sygnalizacji pożarowej czy kontroli dostępu), co przekłada się na wygodne i efektywne zarządzanie bezpieczeństwem.

Agnieszka Pitrus
Head of Marketing SATEL

ZARZĄDZANIE BEZPIECZEŃSTWEM POŻAROWYM W OBIEKTACH WYMAGAJĄCYCH SZCZEGÓLNEJ OCHRONY. SKUTECZNOŚĆ SYSTEMU SYGNALIZACJI POŻARU

System sygnalizacji pożaru. Co to takiego?

System sygnalizacji pożaru (SSP) to podstawowy system zabezpieczający obiekty przed rozprzestrzenianiem się pożaru. Do jego zadań należy wykrycie pożaru, powiadomienie użytkowników obiektu o zagrożeniu, uruchomienie przeciwpożarowych urządzeń wykonawczych oraz wysłanie sygnału o alarmie do jednostki Państwowej Straży Pożarnej. Kompleksowa ochrona obiektu oraz osób w nim przebywających jest uwarunkowana zintegrowaniem tego systemu z innymi systemami bezpieczeństwa np. kontroli dostępu. W łańcuchu urządzeń, to SSP każdorazowo pełni rolę nadrzędną. Sercem SSP jest centrala systemu, która monitoruje stan elementów detekcyjnych oraz wykonuje operacje sygnalizacyjne i sterownicze zgodnie z ustawieniami konfiguracyjnymi. Do wykrywania pożaru służą czujki dymu, ciepła, płomienia oraz elementy wielosensorowe, które jednocześnie analizują różne czynniki pożarowe. Zapewnienie bezpieczeństwa osób i mienia znajdujących się w budynku jest możliwe wyłącznie poprzez odpowiedni dobór rozwiązań technicznych oraz utrzymanie w pełnej sprawności wszystkich elementów tego systemu bezpieczeństwa. Ogólne wytyczne w zakresie planowania, projektowania i instalowania SSP są zawarte w normie PKN-CEN/TS 54-14:2006.

Gdzie jest wymagany system sygnalizacji pożaru

System sygnalizacji pożaru jest bardzo często spotykany w obiektach użyteczności publicznej jednak jego stosowanie jest wymagane tylko w wybranych budynkach, o ściśle określonej charakterystyce.



Rys. 1. Fazy wdrażania skutecznego systemu sygnalizacji pożaru

Kwestia ta została uregulowana w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów. Kwalifikacja danego obiektu do ww. katalogu jest uwarunkowana jego przeznaczeniem, wysokością, powierzchnią stref pożarowych oraz przewidywaną liczbą użytkowników. W katalogu znajdują się m.in. budynki handlowe, wystawowe, do celów gastronomicznych, teatry, kina, sale widowiskowe i sportowe, szpitale, domy pomocy społecznej. Przepisy prawne uwzględniają przede wszystkim budynki, w których występuje znaczne ryzyko zagrożenia zdrowia i życia osób w dużej liczbie. Jednak do obiektów wymagających szczególnej ochrony należą również te, istotne z punktu widzenia zachowania zasobów materialnych dziedzictwa kulturowego i przetwarzania danych np. muzea, biblioteki, archiwa, ośrodki elektronicznego przetwarzania danych, banki.

System Sygnalizacji Pożaru w każdym budynku?

Każdy inwestor, zarządca lub użytkownik obiektu powinien dokonać dokładnej oceny zagrożeń i poziomu zabezpieczeń przeciwpożarowych, niezależnie od warunków określonych w przepisach prawnych. Za obiekty wymagające szczególnej ochrony uznaje się budynki lub ich części, w których przechowywane są przedmioty o znacznej wartości materialnej, informa-

cje lub dobra nieodtworzalne lub takie, których odtworzenie jest bardzo kosztowne. Są to przestrzenie wykorzystywane do elektronicznego przetwarzania danych (serwerownie), pomieszczenia wystawiennicze i magazynowe w muzeach, archiwach, bankach oraz instytucjach państwowych, od których wymagana jest ciągłość działania. W tego rodzaju obiektach należy stosować najskuteczniejsze rozwiązania techniczne w zakresie zabezpieczeń przeciwpożarowych, ponieważ wielkość strat materialnych wskutek wystąpienia pożaru może nieporównanie przewyższyć wydatki związane z zabezpieczeniem się przed ryzykiem. Każdy etap procesu wdrażania SSP wymaga świadomych i konsekwentnych działań.

Pierwszym etapem procesu wdrażania systemu jest analiza ryzyka, oszacowanie potrzeb w zakresie zabezpieczeń oraz przygotowanie koncepcji, która uwzględni:

- czy zabezpieczyć należy cały budynek, czy też jego część;
- rodzaj systemu, który ma być zainstalowany;
- schemat współdziałania instalacji z innymi urządzeniami bezpieczeństwa.

Drugim etapem jest planowanie i projektowanie instalacji, w tym:

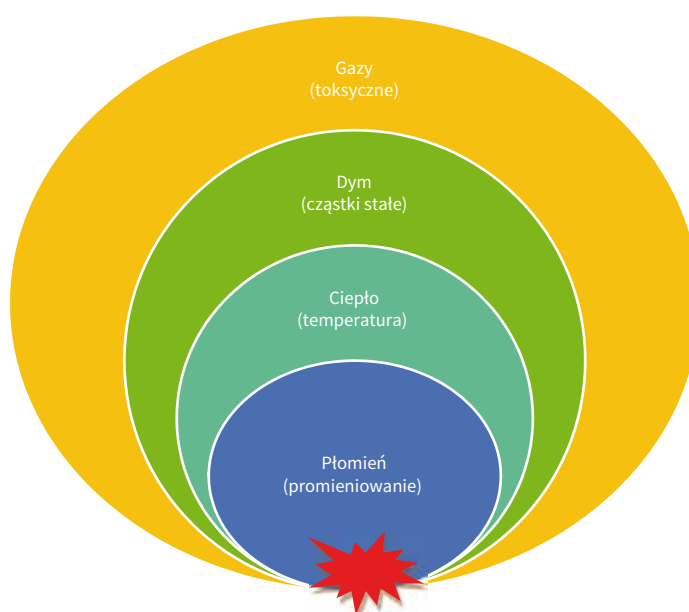
- dobór rodzaju czujek oraz ich rozmieszczenie w różnych częściach budynku;
- podział budynku na strefy dozoru lub alarmowe;
- tryb nadzoru nad instalacją oraz sposób wyświetlania informacji o jej stanie.

Trzecim etapem jest montaż, uruchomienie oraz sprawdzenie prawidłowego działania instalacji. Ostatnim etapem jest eksploatacja i konserwacja. Od każdego z tych etapów zależy uzyskanie oczekiwanej skuteczności.

Dostępne rozwiązania w detekcji pożaru stosowane w systemach sygnalizacji pożaru

Na rynku dostępnych jest wiele rodzajów czujek różniących się budową (czujki punktowe, liniowe, zasysające) oraz zasadą działania. Najczęściej stosowane czujki reagują na dym, ciepło, promieniowanie (płomień) lub występowanie innych symptomów spalania. Od rodzaju czujki zależy szybkość jej reakcji na efekt towarzyszący spalaniu, a tym samym czas niezbędny na wykrycie pożaru. Nie ma czujek uniwersalnych, które byłyby w każdych warunkach jednakowo skuteczne, dlatego tak ważny jest etap planowania i projektowania instalacji. W określonych przypadkach wskazane jest stosowanie czujek różnego rodzaju, a nawet dwóch lub większej liczby niezależnych systemów detekcji. Popularne czujki pożarowe są przeznaczone do wykrywania tylko jednego zjawiska towarzyszącego pożarowi (rys. 2).

Należy zaznaczyć, że nie zawsze wszystkie wyżej wymienione czynniki występują w trakcie pożaru i stąd wy-



Rys. 2. Czynniki towarzyszące pożarowi, na które reagują czujki pożarowe

kają główne ograniczenia w stosowaniu niektórych rodzajów czujek. Poniżej w tabeli 1 przedstawiono charakterystykę typowych czujek pożarowych dostępnych na rynku oraz warunki, w jakich znajdują zastosowanie.

Najczęściej stosowanymi elementami detekcyjnymi w systemach sygnalizacji pożaru są czujki dymu. Wynika to przede wszystkim z faktu, że w większości pożarów podstawowym zjawiskiem jest dym,

a wzrost innych wskaźników pożaru następuje w późniejszej fazie jego rozwoju. W tym kierunku też nastąpił główny rozwój detektorów i powstały czujki dymu zasysające. W przeciwieństwie do standardowych czujek, instalacja taka zbudowana jest z sieci rurek zasysających, przez które stale przetłaczane jest powietrze pochodzące z wybranych przestrzeni monitorowanego pomieszczenia. Czujnik może być w tym przypadku oddalony od

Czujka ciepła	- reaguje na niestandardową temperaturę i/lub szybkość jej narastania lub różnice, - skutecznie wykrywa pożary, w trakcie których szybko wywołuje się ciepło przy niewielkiej ilości dymu - nie wolno ich stosować w miejscach, w których przekraczane są parametry ich pracy określone przez producenta, występuje niebezpieczna chemicznie atmosfera lub pył, nie nadają się do zastosowań zewnętrznych
Czujka promieniowania (płomienia)	- reaguje na promieniowanie emitowane przez płomień, skutecznie wykrywa pożary cieczy palnych - może być stosowana na zewnątrz lub w bardzo wysokich pomieszczeniach - ma ograniczone zastosowanie w przestrzeniach, w których występuje produkcja lub inne procesy wywołujące promieniowanie oraz wykazuje brak zdolności wykrywania pożarów bezpłomieniowych
Czujka dymu optyczna	- reaguje na zjawiska pochłaniania i rozpraszania światła, reaguje szybciej na większe cząstki gęstego dymu - nie nadaje się do zastosowań zewnętrznych i bardzo wysokich pomieszczeń - nie powinna być stosowana w miejscach, w których w warunkach normalnych powstaje dym, pył oraz pary
Czujka dymu jonizacyjna	- reaguje na produkty spalania wpływające na prąd jonizacji w jej komorze, w szczególności cząstki o małej wielkości zawarte w dymie - może nie wykryć produktów spalania cieczy palących się bez dymu - nie powinna być stosowana w miejscach, w których w warunkach normalnych powstaje dym, pył oraz pary
Liniowa czujka dymu	- reaguje na osłabienie wiązki światła w dymie, jest bardziej czuła na średnią wartość gęstości dymu - jest jedynym rodzajem czujki dymu mającą zastosowanie w wysokich pomieszczeniach - ma ograniczone zastosowanie w niskich przestrzeniach, w których może odbywać się ruch oraz występuje pył, pary oraz dym
Czujka wielosensorowa	- stanowi kombinację dwu lub więcej rodzajów czujek, z których przetwarza odpowiednio sygnały - poprzez odpowiedni algorytm ma możliwość ograniczenia alarmów fałszywych - ich ograniczenia są analogiczne do czujek, z których elementów detekcyjnych się składają

Tabela 1. Ogólna charakterystyka zastosowania typowych czujek pożarowych



> Centrala sterująca i monitorująca
dowolne urządzenia ochrony
przeciwpożarowej



FPM+
Fire Protection Manager steruje:

Przeciwpożarowe klapy odcinające
Windy, schody ruchome i trawelatory
Drzwi z kontrolą dostępu
Wyjścia ewakuacyjne
Wentylatory przeciwpożarowe
Centrale sygnalizacji pożarowej
Konwencjonalne czujki pożarowe
Przyciski RPO i ROP
Czujniki ciśnienia, temperatury,
kierunku i siły wiatru, obecności napięcia

Trzymacze (zwalniaki) elektromagnetyczne
Systemy DSO
Stałe urządzenia gaśnicze
Inne urządzenia automatyki budynkowej
Styczniki, falowniki, przełączniki
Klapy odcinające, dymowe, kurtyny
dymowe itp.

www.ela.pl

chronionego obszaru, przez co nie jest bezpośrednio narażony na czynniki szkodliwe. Powietrze po przefiltrowaniu jest analizowane przez urządzenie detekcyjne, pozwalające na wykrycie nawet najdrobniejszych cząstek dymu. Detektory tego typu, znacznie wcześniej potrafią wykryć cząstki spalających się substancji w stosunku do czujek konwencjonalnych. Ich czułość może być ponad 100 razy większa. Wśród dostępnych rozwiązań nieomawianych wcześniej znajdują się czujki gazu, które są zdolne wykryć gazy towarzyszące spalaniu takie, jak CO, CO₂, NH₃ i interpretować ich obecność jako pożar. Ten typ detektorów stosowany jest stosunkowo rzadko.

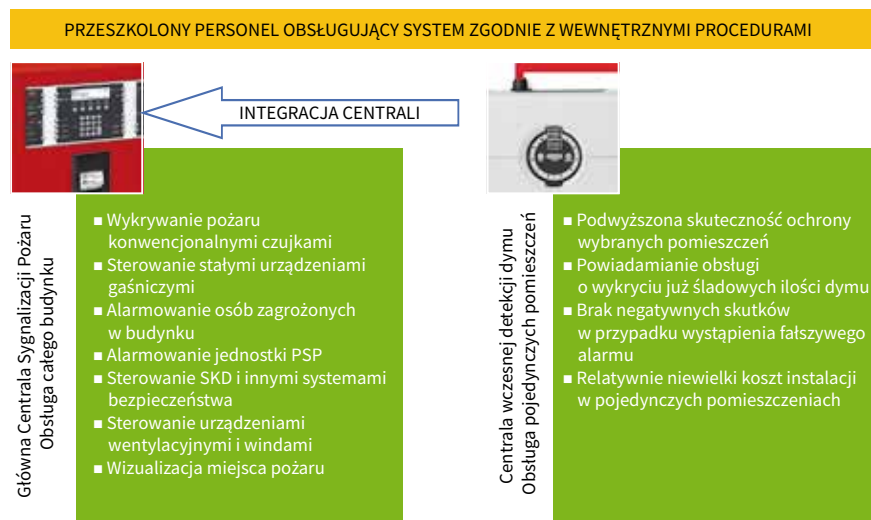
Skuteczny systemy sygnalizacji pożaru

Chcąc zbudować skuteczny system sygnalizacji pożaru musimy przeprowadzić szczegółową analizę zagrożeń, warunków przebiegu spalania typowego wyposażenia i dokonać wyboru odpowiednich urządzeń oraz elementów detekcyjnych. Odpowiednio dobrane czujki powinny zapewnić możliwie wcześnie i niezawodne alarmowanie, dostosowane do specyfiki zagrożeń w przestrzeni chronionej. Od skutecznego systemu sygnalizacji pożaru oczekiwana jest niezawodność, duża czułość elementów detekcyjnych i ich wysokie zabezpieczenie przed generowaniem alarmów fałszywych. Możliwych kombinacji rozwiązań jest bardzo wiele, dlatego każdy przypadek należy rozpatrywać indywidualnie. Niewłaściwy dobór i montaż elementów detekcyjnych może sprawić, że nawet najdroższe urządzenie wykrywające pożar może nie zadziałać z oczekiwaną skutecznością. W obiektach wymagających szczególnej ochrony należy unikać stosowania uniwersalnych i budżetowych rozwiązań, gdyż mogą się nie sprawdzić w sytuacji wystąpienia zagrożeń. Przy projektowaniu należy uwzględnić warunki lokalne panujące stale lub mogące wystąpić w chronionej przestrzeni. Czynnikiem wymagającym uwzględnienia jest chociażby praca urządzeń wentylacyjnych i klimatyzatorów. Ponadto, zaprogramowane w czujkach algorytmy eliminacji alarmów fałszywych wydłużają czas na wywołanie zdarzenia w systemie. To również w praktyce oznacza wydłużenie czasu swobodnego rozwoju pożaru, któremu towarzyszyć może już powstawanie znacznych zniszczeń w wyposażeniu i strat. Z drugiej strony zbyt wysoka czułość

może sprawić, że będzie dochodziło do częstych alarmów fałszywych, które mogą zakłócić funkcjonowanie obiektu, generować przy tym koszty i obniżyć zaufanie do urządzeń oraz zmniejszyć responsywność personelu na zdarzenia w systemie. Jednym z rozwiązań tego problemu mogą być dwa niezależne systemy detekcji pracujące równolegle. Kluczem do ich skutecznego powiązania jest programowanie i przypisanie urządzeniom odpowiednich funkcji. Za przykład posłużyć może niewielkie pomieszczenie przeznaczone na serwerownię. W przypadku tego typu pomieszczeń stosowanie czujek płomienia nie jest wskazane z uwagi na sposób spalania przebiegający w urządzeniach elektronicznych a czujek ciepła – z uwagi na intensywnie działające urządzenia klimatyzacyjne. Detekcja pożaru oparta zasadniczo na czujkach punktowych dymu, w przypadku małych pomieszczeń klimatyzowanych w wielu przypadkach nie zapewni ich odpowiednio szybkiej reakcji przez wpływ wentylacji na detekcję. Nieprawidłowe umieszczenie czujek pożarowych dymu w stosunku do przewodów wentylacji i klimatyzacji pomieszczeń może doprowadzić do utrudnienia dostępu dymu do tych elementów przez powietrze wypływające z systemu wentylacyjnego. Rozwiązanie to sprawdzi się do generowania alarmu pożarowego I i II stopnia oraz sterowania urządzeniami automatycznymi w budynku i rozgłaszanie komunikatów o zagrożeniu. Równolegle obok tego systemu dla zwiększenia skuteczności ochrony pojedynczego pomieszczenia można zastosować system wczesnej detekcji dymu generujący sygnał o zagrożeniu do obsługi budynku.

Odpowiednio wcześnie alarmowanie pozwoli, by pracownicy mogli w porę rozpoznać zagrożenie w jak najwcześniejszej fazie, ocenić je na miejscu i podjąć działania gaśnicze dostępnym sprzętem lub jeśli zachodzi taka konieczność użyć ręcznego ostrzegacza pożarowego uruchamiając procedurę alarmu II stopnia. Duża czułość mogąca w pewnych warunkach skutkować alarmami fałszywymi w tym przypadku nie będzie zauważalna dla innych użytkowników budynku.

Koszt wyposażenia pomieszczenia w skuteczny system detekcji jest zdecydowanie niższy w porównaniu do adekwatnego systemu gaszenia. Sprawnie działający system detekcji pozwala zareagować pracownikom w budynku zanim konieczne będzie użycie systemów gaszenia. Poza tym nawet najlepszy system gaszenia bez odpowiedniej detekcji nie będzie w pełni skuteczny. To tylko przykładowa konfiguracja, którą można zastosować w niewielkim pomieszczeniu serwerowni. W innych przypadkach wybór rozwiązania może być zupełnie inny. Oprócz szybkiej detekcji pożaru kluczowe dla skuteczności ochrony jest szybkie zidentyfikowanie pomieszczenia lub przestrzeni, gdzie doszło do pożaru. Rozwiązaniem, poprawiającym komfort obsługi systemu sygnalizacji pożaru są systemy komputerowej wizualizacji rozmieszczenia elementów detekcyjnych. Sprawdzają się one w dużych obiektach o skomplikowanym układzie przestrzennym. System wizualizacji potrafi wyświetlić miejsce pożaru i przez to szybciej zadziałać obsługa systemu. W dobie cyfryzacji stworzenie wizualizacji przestrzennych nie stanowi większego problemu. System sygnalizacji



Rys. 3. Schemat ideowy zaproponowanego rozwiązania

pożaru, jako urządzenie przeciwpożarowe podlega obowiązkowym przeglądom. Poza kosztami wykonania systemu to kolejny koszt związany z utrzymaniem, na którym nie warto oszczędzać, zwłaszcza w obiektach wymagających szczególnej ochrony. W ostatnim etapie utrzymania skuteczności zainstalowanych urządzeń poza konserwacją jest właściwy nadzór nad ich pracą. Kluczowe jest powierzenie nadzoru wykwalifikowanemu personelowi pracującemu w systemie całodobowym oraz wdrożenie wewnętrznych procedur w oparciu, o które działać będą wyznaczeni pracownicy lub wewnętrzne służby ochrony.

Podsumowanie

Wraz z rozwojem wiedzy i techniki w ochronie przeciwpożarowej stosowane są coraz skuteczniejsze rozwiązania. W przypadku dostępności całodobowego, wykwalifikowanego personelu wyposażonego w podręczny sprzęt gaśniczy, organizację ochrony przeciwpożarowej w budynku można dodatkowo usprawnić poprzez montaż wysokoczułych urządzeń wczesnej detekcji pożaru. Jest to stosunkowo nowatorskie rozwiązanie, jednak wystarczająco sprawdzone i doceniane. System wczesnej detekcji przede wszystkim pozwala na bezzwłoczne powiadomienie personelu dyżurującego o możliwej sytuacji pożarowej, co pozwala na podjęcie działań zapobiegawczych eliminujących ryzyko poniesienia jakichkolwiek strat materialnych bez uruchamiania instalacji gaśniczych. Dla podjęcia skutecznych działań równie ważna jest błyskawiczna identyfikacja i dotarcie do strefy, w której został wykryty pożar. W tym zakresie, wsparciem dla służb i operatorów obiektu jest komputerowa wizualizacja systemu sygnalizacji pożaru z uwzględnieniem rozmieszczenia i stanu elementów detekcyjnych. Rozwiązanie to jest szczególnie przydatne w dużych obiektach ze skomplikowaną strukturą przestrzenną i rozbudowanym, elektronicznym systemem bezpieczeństwa. O wysokiej skuteczności systemu sygnalizacji pożaru decyduje właściwa analiza zagrożeń, odpowiedni dobór rozwiązań technicznych, ale również kompetencje i umiejętności operatorów systemu, dla których wsparciem są właśnie systemy wizualizacji. ■

Wykorzystano:

1. PKN-CEN/TS 54-14:2006 Systemy sygnalizacji pożarowej Część 14: Wytyczne planowania, projektowania, instalowania, odbioru, eksploatacji i konserwacji
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 roku (Dz. U. z 2010 r. nr 109, poz. 719 z późn. zmianami)

st. kpt. mgr inż. Krzysztof Majdak

Absolwent Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej w Warszawie oraz podyplomowych studiów Politechniki Warszawskiej w zakresie bezpieczeństwa i higieny pracy. Od początku swojej drogi zawodowej związany z Państwową Strażą Pożarną.

Doświadczenie zdobywał w pionie kontrolno – rozpoznawczym ukierunkowanym na rozpoznawanie zagrożeń pożarowych w obiektach, a także w pionie operacyjnym, będąc odpowiedzialnym za kierowanie działaniami ratowniczo-gaśniczymi. Przez kilka lat wykonywał obowiązki na stanowisku związanym z ochroną przeciwpożarową obiektów handlowych, a obecnie specjalizuje się w zarządzaniu bezpieczeństwem pożarowym w budynkach muzealnych. Jednym z jego osobistych zainteresowań jest ochrona dóbr kultury na wypadek szczególnych zagrożeń, które łączy z pracą zawodową."

Reklama







SLIM LINE

Nowa rodzina czujek ruchu

- ✓ 5 modeli PIR oraz 5 dualnych (PIR + MW)
- ✓ wysoka skuteczność wykrywania ruchu – nowy algorytm detekcji, unikalna soczewka, mechanizm kompensacji temperatury
- ✓ rozwiązania konstrukcyjne umożliwiające wygodny i szybki montaż
- ✓ zdalne konfigurowanie parametrów pracy czujki
- ✓ wybór koloru świecenia wskaźnika LED – dostępnych 7 barw



Dowiedz się więcej:
www.satel.pl/extra/slim-line

www.satel.pl

PRZYGOTOWANIE STANOWISKA OPERATORA SYSTEMU DOZORU WIZYJNEGO

ASPEKTY PSYCHOLOGICZNE I TECHNICZNE

*Jeżeli jakąś czynność
uznajemy za łatwą lub
naturalną, mamy tendencję
do lekceważenia złożoności
układów, dzięki której jest
ona możliwa¹.*

Dlaczego obserwacja w systemie dozoru wizyjnego stwarza tyle trudności?

Towarzyszący nam od urodzenia zmysł wzroku oraz możliwość orientacji przestrzennej sprawiają, że nie zastanawiamy się nad złożonością mechanizmu związanego z widzeniem otaczającego świata, nie wspominając o rozpoznawaniu rzeczy znanych, wyszukiwaniu szczegółów i dostrzeganiu rozbieżności z dotychczasowymi doświadczeniami. Wszystko to dzieje się automatycznie w ułamkach sekund, dlatego powstaje przeświadczenie, że w zakresie percepcji wizualnej można wykonywać wiele rzeczy jednocześnie. Jednak wielozadaniowość ludzkiego mózgu to złudzenie, gdyż jak wykazują badania, mózg może się skupić wyłącznie na jednym zadaniu przy jednoczesnym śledzeniu od 3 do 6 podobnych obiektów znajdujących się w obszarze widzenia² oraz do 6 różnych kierunków poruszania się podobnych obiektów³. Jest to cecha ludzkiego mózgu, a dokładniej umysłu, który buduje swój obraz otaczającej rzeczywistości od dzieciństwa, uczy się modeli obiektów,

z których sukcesywnie składa postrzegany obraz świata. Kiedy zna modele uzupełnia je na bieżąco tylko niewielkimi fragmentami informacji i tworzy to, co w danej chwili widzi (między innymi dlatego widzimy stabilny obraz mimo ruchu oczu i głowy). Jeżeli natomiast nie znamy modelu tego, na co patrzymy, potrzebujemy więcej czasu na skupienie uwagi, ażeby widzieć – dostrzec i rozpoznać, czyli porównać z dotychczasowym doświadczeniem. Mózg uczy się wybierania istotnych i pomijania nieistotnych bodźców, dlatego samo skierowanie wzroku na obiekt nie świadczy jeszcze o tym, że coś widzimy⁴. **Innymi słowy to, że na coś patrzymy wcale nie gwarantuje, że to coś zobaczymy⁵.** Kiedy dostrzega tylko to, czego nauczył się wcześniej postrzegać lub kieruje uwagę tam, gdzie znajdzie odpowiedź na pojawiające się w umyśle pytanie⁶. Nie ma uniwersalnej metody postrzegania rzeczywistości, ponieważ każdy doświadcza inaczej sygnałów dostarczanych od urodzenia przez zmysły. Umysł wykorzystuje efekt uczenia się i rozpoznawania obrazów tworzących pewien schemat w celu optymalizacji pracy mózgu i oszczędności zasobów energetycznych potrzebnych do procesów poznawczych. Mózg przede wszystkim reaguje na zmiany i uaktywnia się w sytuacjach, kiedy dostrzegany obiekt odbiega od doświadczenia zmysłowego i dotychczasowych schematów. Pojawiający się dysonans poznawczy wymaga uruchomienia świadomych procesów uwagi dowolnej, procesów pamięciowych, analizy i syntezy myślenia, a także

innych. To właśnie wewnętrzne modele rzeczywistości stanowią podstawę do świadomej percepcji, która uruchamiana jest szczególnie, gdy rzeczywistość nie pasuje do obecnego w umyśle schematu. Należy dodać, że ludzka percepcja jest procesem wielopoziomowym, w którym uczestniczą różne zmysły⁷, dlatego obserwacja na stanowisku operatora systemu dozoru wizyjnego jest trudna i obciążona dużym wysiłkiem. Na tym stanowisku aktywny jest bowiem wyłącznie zmysł wzroku, a dodatkowym utrudnieniem jest konieczność przetwarzania w umyśle obrazu płaskiego widniejącego na monitorze w obraz przestrzenny, co wymaga procesów analizy bodźców płynących z obrazu i ich syntezy w spostrzeżenia odpowiadające rzeczywistości trójwymiarowej.

Niestety ulegamy złudzeniom, a w konsekwencji przeceniamy swoje możliwości dotyczące spostrzegania, stąd biorą się rozczarowania, co do efektywności operatora systemu dozoru wizyjnego. To także konsekwencja pewnego błędu myślowego wywodzącego się z dziedziny, jaką jest automatyka a związanego z HMI (ang. *Human Machine Interface* lub MMI ang. *Man Machine Interface*, HCI ang. *Human Computer Interface*). Uproszczając definicję powyższych, jest to element urządzenia – oprogramowania, pozwalający realizować interakcję człowieka z maszyną i maszyny z człowiekiem⁸. Jak potwierdzają badania⁹ pomiędzy HMI/MMI/HCI a człowiekiem występuje jeszcze jeden istotny interfejs, jakim jest percepcja. Ten interfejs (rys. 1.) ma co najmniej równorzędną znaczenie dla całego systemu dozoru wizyjnego, co całość zagadnień technicznych. Twórcy oprogramowania uwzględniają percepcję

¹ D. Eagleman, *Mózg incognito. Wojna domowa w Twojej głowie*, PWN, Warszawa 2013, s. 60–154.

² D. Bavelier, *Your brain on video games*, wykład online [źródło internetowe: https://www.ted.com/talks/daphne_bavelier_your_brain_on_video_games/transcript?utm=; dostęp: 06.07.2019].

³ Serial, *National Geographic Pułapki umysłu*, sezon 3, odc.9

⁴ Serial BBC Earth HD USA 2015: *Tajemnice ludzkiego mózgu*, odc. 1.

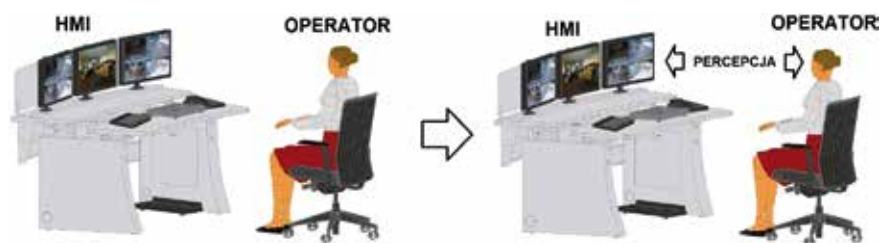
⁵ D. Eagleman, *Mózg incognito* ... op. cit.,

⁶ R. Nakayama, I. Motoyoshi, *Attention periodically binds visual features as single events depending on neural oscillations phase-locked to action*, "Journal of Neuroscience", 2019, 39 (21), s. 4153–4161 [źródło internetowe: <https://doi.org/10.1523/JNEUROSCI.2494-18.2019>]; dostęp: 06.07.2019].

⁷ D. Eagleman, *Mózg incognito* ... op. cit.

⁸ Definicja ze źródła internetowego [www.techopedia.com; dostęp: 28.07.2019 r.]

⁹ H. Ashbach, *The case against reality*, UCI School of Social Science, 22.07.2019 r.



Rys. 1. Percepcja jako interfejs użytkownika

Źródło: Opracowanie własne

w tzw. *user experience* (ang. *UX*), definiowanym jako doświadczenia użytkownika podczas interakcji z produktem, usługą, środowiskiem lub obiektem¹⁰.

Widzenie jest skomplikowanym procesem, który dzieli się na etapy. Pierwszym etapem jest odbiór wrażenia, czyli pobudzenie receptora i przekazanie informacji drogami nerwowymi do dalszych struktur mózgowych celem poddania ich obróbce poznawczej. Większość bodźców jednak nie będzie docierała do świadomości obserwatora, gdyż każdy człowiek ma indywidualny próg wrażliwości sensorycznej, poniżej którego nie reaguje na bodźce. Oprócz progu wrażliwości decydujące znaczenie w odbiorze bodźców wzrokowych ma również stymulacja innymi bodźcami w tle oraz sprawność detektorów, czyli wzajemnie powiązanych struktur mózgowych. Następnie odebrany bodźcom nadawane jest znaczenie (przetworzenie wrażenia w spostrzeżenie) poprzez proces spostrzegania, czyli nadawania znaczenia bodźcom w oparciu o obecne w umyśle wspomnienia, emocje, motywy i inne wyuczone skojarzenia np. zaobserwowana mimika twarzy, nerwowość w poruszaniu się, gesty itp. Dalsze przetwarzanie percepcyjne polega na łączeniu odebranych aktualnie spostrzeżeń ze zmagazynowanymi w pamięci wspomnieniami i doświadczeniami. Pozwala to na rozpoznawanie i różnicowanie osób, przedmiotów oraz ocenę sytuacji. Uwzględnienie tych procesów wpływa na określenie parametrów stanowiska obserwatora związanych między innymi z wielkościami obiektu w obrazie czy odległości obserwatora od monitora w zależności od rodzaju obserwacji (ogólnej i szczegółowej)¹¹. Opisane przetwarzanie bodźców

na poziomie sensorycznym (zmysłowym) uzależnione jest w dużej mierze od właściwości psychofizycznych obserwatora i stworzonych optymalnych warunków ergonomicznych stanowiska obserwacji. Jednak bardziej skomplikowane operacje percepcyjne i idące za nimi odpowiednie decyzje są uzależnione od motywacji, zaangażowania oraz procesów uczenia się i treningu. Percepcja, czyli przetwarzanie wrażeń w spostrzeżenia obejmuje dwa rodzaje procesów przetwarzania: przetwarzanie odgórne – kierowanie uwagi na określony obiekt oraz przetwarzanie oddolne – reagowanie na pojawiające się bodźce, bez wcześniejszego nastawienia. Obserwator odpowiednio przygotowany – wytrenowany, szybciej zareaguje na bodźce spełniające kryteria obserwacji lub odbiegające od normy, na zasadach przetwarzania odgórnego. Niestety może pominąć większość bodźców niespełniających jego nastawień. Z kolei w percepcji oddolnej obserwator nie wyszukuje bodźców, tylko reaguje na te, które są w polu widzenia. Obydwa procesy przeplatają się, a każdy z nich ma swoje zalety (np. właściwa reakcja) i wady (np. pominięcie zdarzenia). Realizacja zadań na stanowisku operatora dozoru wizyjnego, oprócz predyspozycji psychofizycznych i odpowiedniego wytrenowania, wymaga zaangażowania i świadomego skierowania strumienia uwagi na obserwowane monitory oraz oceny tego, co jest na nich aktualnie wyświetlane. Jednocześnie w trakcie realizacji tych czynności mogą pojawić się nieoczekiwane inne bodźce (dystraktory) zakłócające te czynności, które mimowolnie odciągną uwagę obserwatora. Procesy uwagi (dowolnej, czyli świadomej kierowanej oraz mimowolnej, czyli odruchowej) posiadają kilka cech i właściwości (koncentracja, selektywność, przerzutność, podzielność, trwałość, stałość), które uzależnione są od indywidualnych właściwości osobniczych i zmieniają się pod wpływem okoliczności i kontekstu sytuacyjnego. **Nie wystarczy zatem samo zaprojektowanie stanowiska i wyposażenie go w naj-**

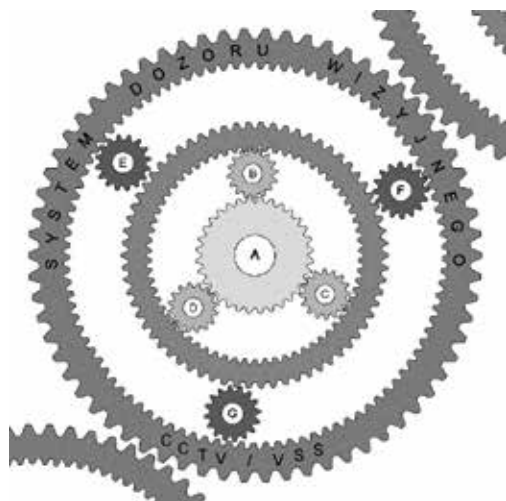
nowszą technologię, ale konieczna jest odpowiednia selekcja operatorów oraz ich odpowiednie szkolenie, które po pierwsze nauczy ich właściwej oceny sytuacji i podejmowania odpowiednich decyzji, a po drugie wpłynie na kształtowanie ich motywacji do bardziej świadomego kierowania strumieniem uwagi i przewidywania zdarzeń na podstawie wczesnych sygnałów zbliżającego się niebezpieczeństwa¹². Te ustalenia zawiera norma PN-EN 50518-3 pkt 4.3 w stwierdzeniu, że nowy operator systemu powinien mieć asystę doświadczonego operatora, zanim samodzielnie podejmie pracę na stanowisku. Szczególnie ważna jest selekcja kandydatów na operatorów systemu dozoru wizyjnego, gdyż nie każdy nadaje się na to stanowisko. Nie tylko dlatego, że ma zbyt wysoki poziom wrażliwości na bodźce wzrokowe (nie reagowanie na bodźce o małej intensywności), ale dlatego, że jest podatny na zjawisko tzw. ślepoty z nieuwagi (w literaturze spotyka się też określenia „ślepotą z braku uwagi”, „ślepotą przez nieuwagę” czy „ślepotą pozauwagową”). Zjawisko to polega na tym, że koncentracja na jednym zadaniu np. obserwacji określonego obrazu i oczekiwanie na określony rodzaj bodźców, powoduje, że mimo zmian warunków obserwacji lub pojawienia się innego bodźca (w obrazie) nie jest on zarejestrowany w świadomości obserwatora. **Przeprowadzone przez autorów niniejszego opracowania badania nad tym zjawiskiem (tzw. efekt goryla) wśród personelu więziennego ujawniły, że tylko połowa funkcjonariuszy biorących udział w badaniu wykazała się właściwą czujnością i dokładnością percepcji, na tyle, żeby wykonać zadanie, blisko 40% funkcjonariuszy nie zauważyło intruza, który wtargnął w miejsce obserwacji, zaledwie 10% odnotowało zniknięcie jednej osoby z pola widzenia oraz około 5% zaobserwowało zmiany warunków obserwacji¹³.** Uzyskane w tym badaniu wyniki mają szczególne znaczenie w związku z próbami samobójczymi i samobójstwa-

¹² Zainteresowanych czytelników odsyłamy do artykułu C. Mecwaldowski, R. Poklek, *Psychologiczne i techniczne aspekty stanowiska operatora dozoru wizyjnego. Część 2: Percepcja i uwaga w pracy obserwatora*, „SEC&AS”, 2019, nr 2, s. 46–51.

¹³ Por. R. Poklek, C. Mecwaldowski, *Video surveillance of prisoners in Polish Prison Service. Observer's perspective*, „Journal of Humanities and Social Science”, 2018, vol. 23, issue 2, s. 31–42; [źródło internetowe: https://www.researchgate.net/publication/323539340_Video_surveillance_of_prisoners_in_Polish_Prison_Service_Observer's_perspective; dostęp: 06.07.2019].

¹⁰ M. Hassenzahl *User Experience (UX): Towards an experiential perspective on product quality* [dostęp: www.marc-hassenzahl.de 28.07.2019 r.]

¹¹ Zainteresowanych czytelników odsyłamy do artykułu C. Mecwaldowski, R. Poklek, *Psychologiczne i techniczne aspekty stanowiska operatora dozoru wizyjnego. Część 1: Wrażenia i spostrzeganie*, „SEC&AS”, 2019, nr 1, s. 47–51.



LEGENDA

Obszar techniczny (bez operatora):

- A** System dozoru wizyjnego wykonany bez uwzględnienia norm i wiedzy technicznej
B System dozoru wizyjnego, z uwzględnieniem norm, ale bez testów
C Precyzyjnie określony cel stosowania systemu, wykonane testy systemu i sprawdzone procedury
D Integracja systemu dozoru wizyjnego z innymi systemami (ang. Integrated Systems), analiza wizyjna (ang. Video Content Analysis – VCA), sztuczna inteligencja (ang. Artificial Intelligence – AI)

Obszar osobowy (z operatorem):

- E** Selekcja operatora ze względu na predyspozycje
F Szkolenia operatora: stanowiskowe, specjalistyczne, doskonalące; kompetencje operatora: wiedza, umiejętności, motywacja i zaangażowanie
G Ergonomia stanowiska

Rys. 2. Schemat funkcjonalny systemu dozoru wizyjnego, jako jedna ze składowych systemu bezpieczeństwa

Źródło: opracowanie własne

mi osadzonych w celach monitorowanych oraz związaną z tym odpowiedzialnością dyscyplinarną i karną funkcjonariuszy Służby Więziennej, pełniących służbę na stanowiskach „monitorowych”.

System dozoru wizyjnego jako składowa systemu bezpieczeństwa obiektu

System dozoru wizyjnego może pełnić różne funkcje: od prostej rejestracji sygnału wizyjnego po przeciwdziałanie zdarzeniom, zarówno w zakresie bezpieczeństwa obiektów lub obszarów, jak i procesów przemysłowych. System dozoru wizyjnego jest składową systemu bezpieczeństwa. Może stanowić skomplikowany układ zależności rys. 2, w której każda składowa jest bardziej lub mniej istotna, a jej rola wynika z celu stosowania systemu i przeprowadzonej analizy ryzyka w procesie zarządzania ryzykiem.

Autorzy skłaniają się ku podziałowi na składowe zależne w obszarze technicznym i osobowym. Są one we wzajemnych relacjach wpływających na efektywność całego systemu dozoru wizyjnego.

W literaturze można znaleźć systemowe zależności w innym ujęciu niż opisane

powyżej. Różnice dotyczą zakresu i priorytetu zarówno obszaru technicznego, jak i osobowego, szczególnie w przypadku dotyczącym monitoringu miejskiego¹⁴. Zastosowane rozwiązania w poszczególnych obszarach zależne są od przeprowadzonej analizy ryzyka. W obszarze technicznym będzie to np. określony stopień systemu (ang. *Grade*)¹⁵. W obszarze osobowym, analiza ryzyka wymusi odpowiednie wymagania ergonomii i konstrukcji stanowiska wraz z procedurami w celu osiągnięcia maksymalnej efektywności pracy operatora. Pojęcie skali ryzyka rozpatrywanego przy tworzeniu systemu dozoru wizyjnego, przekłada się bezpośrednio na jego efektywność, jest odwrotnie proporcjonalne. W skrajnym przypadku wynik analizy ryzyka w połączeniu z koniecznością poniesienia niezbędnych kosztów, może wskazać na korzyść innego rozwiązania niż zastosowanie systemu dozoru wizyjnego¹⁶.

¹⁴ P. Wittich, *Zarządzanie systemowe w miejskim systemie monitoringu*, „A&S”, 2017, nr 3.

¹⁵ PN-EN 62676: Systemy dozoru wizyjnego stosowane w zabezpieczeniach.

¹⁶ W. Więckowski, *Czego systemy dozoru wizyjnego wymagają od transmisji wizji IP i dlaczego nie spełnia tych wymagań?*, „SEC&AS”, 2019, nr 1.

Przygotowanie stanowiska operatora dozoru wizyjnego

Przystępując do projektowania systemu, projektant jest doradcą inwestora¹⁷. Szczegółowe określenie celu stosowania systemu dozoru wizyjnego jest niezbędne do jego prawidłowego zaprojektowania¹⁸. Uzgodnienia obejmują przede wszystkim zakres stosowania systemu:

- Bezpieczeństwo obszaru lub obiektu, wsparcie automatyki obiektu, nadzór nad procesem przemysłowym (SCADA), obserwacja obrazów ze skanerów X-Ray, obserwacja obrazów z dronów, radarów itp.;
- Zastosowanie VCA, AI;
- Zapis sygnału wizyjnego (funkcja wodowa) lub bez zapisu;
- Zintegrowanie lub nie z innymi systemami obiektu, obszaru;
- System bez operatora lub z operatorem;
- Wymóg przeciwdziałania zdarzeniom bądź wyłącznie przeciwdziałanie ich skutkom, itp.

Powyższe założenia wpisują się w zarządzanie ryzykiem i związane są z poziomem ryzyka, czyli skutkiem jaki przyniesie niezrealizowanie założonego celu (kradzieże, zniszczenie mienia, wtargnięcie do obiektu, obszar, problemy komunikacyjne, katastrofy, przemyt, po zabójstwa lub samobójstwa osób dozorowanych). Wskazane cele opisuje się wraz z procedurami ich realizacji w dokumencie „Wymagania użytkowe” (ang. *Operational Requirement OR*)¹⁹ łącznie z wymaganiami stawianymi operatorom i ich szkoleniom.

Ile obrazów z kamer powinien oglądać jeden operator?

Należy tutaj rozróżnić liczbę obrazów od liczby monitorów, ponieważ nie są one tożsame. Na monitorze można uzyskać różne podziały obrazu. Istotną rolę odgrywa też liczba obserwowanych scen, przy czym scenę rozumiemy jako pogrupowane logicznie i znaczeniowo obrazy: obszary ulicy, pasy ochronne w ochronie obwodowej, korytarze, przejścia itp., związane z celem monitorowania. Współczesne badania wskazują na przewagę teorii obser-

¹⁷ W. Więckowski, *Artykułowanie potrzeb przy planowaniu, projektowaniu i wdrażaniu systemów dozoru wizyjnego*, „SEC&AS”, 2018, nr 3, s. 35.

¹⁸ C. Mecwaldowski, *Dozór wizyjny wykorzystujący technologię IP. Konsekwencje stosowania*, „SEC&AS”, 2018, nr 5.

¹⁹ PN-EN 62676: Systemy dozoru wizyjnego stosowane w zabezpieczeniach.

wowanych scen nad obrazami, w kontekście percepcji obserwatora. Autorzy także skłaniają się ku liczbie obserwowanych scen szczególnie, kiedy wprowadzane są nowe technologie wyświetlania obrazów, ekranów wielkogabarytowych LED, skalowania i procesorów obrazu itp. Niektóre źródła podają, że maksymalna liczba to 12–16 obrazów z kamer przypadających na jednego operatora. To maksymalna liczba pozwalająca uzyskać akceptowalną efektywność, przy niskiej złożoności zadań operatora²⁰. Publikowane w Internecie badania wskazują jednoznacznie:

- Efektywność obserwacji wzrasta wraz z malejącą liczbą obrazów do obserwacji (w skrajnym przypadku obraz będzie jeden np. operator radaru na lotnisku);
- Podział ekranu na wiele obrazów/scen niesie ograniczenia w dostrzeganiu obiektów, ich wielkości w danym obrazie (dla pojedynczego obserwowanego obrazu, wielkość obiektu w tym obrazie wraz z parametrami percepcji obserwatora podaje norma PN-EN 62676-4). Operatorzy dla jednego monitora preferowali podział 1–4, przy wzroście liczby obrazów dla podziału 4–9 wzrastała też liczba niewykrytych zdarzeń;
- Wzrost liczby obserwowanych monitorów ma drastyczny wpływ na pogorszenie efektywności obserwacji: 1 monitor – 85%, 4 monitory – 74%, 6 – 58%, 9 – 53%²¹;
- Złożoność obserwowanego obrazu często nie jest uwzględniana przy obciążeniu zadaniowym operatora, a ma to kluczowe znaczenie do osiągnięcia celu obserwacji i czasu reakcji operatora – oczekiwanej efektywności;
- Należy wziąć pod uwagę zakres widzenia centralnego i peryferyjnego.

Z jakiej odległości operator powinien obserwować obrazy na monitorach?

Stosuje się odmienne zasady określania odległości obserwacji w zależności od przeznaczenia monitorów/ekranów. Należy rozróżnić ich dwa rodzaje:

1. Ściana monitorów (ang. *Video-wall, Monitor bank* itp) przeznaczone do

obserwacji ogólnej, często do wymiany informacji pomiędzy wieloma operatorami.

2. Monitory stanowiskowe, szczegółowe lub incydentalne (ang. *Workstation or Incidental/spot monitor*) przeznaczone do szczegółowej, zadaniowej obserwacji.

Przez wiele lat funkcjonowania analogowych systemów dozoru wizyjnego, z obrazem PAL, dla uproszczenia obliczeń odległości obserwacji przyjmowano wielokrotność przekątnej ekranu. Kiedy pojawiły się rozwiązania cyfrowe, różne proporcje ekranów i rozdzielczości, obliczenia odległości nieco się skomplikowały²². Jeżeli odległość lub kąt obserwacji znajdują się poza parametrami wzroku, wielkość obiektu w obrazie nie spełnia kryteriów bodźca, a efektywność obserwacji staje się skrajnie niska – prawdopodobieństwo przeoczenia zdarzenia wysokie²³.

W wielu źródłach odnaleźć można przelicznik odległości obserwacji, która wynika z rozdzielczości ludzkiego oka oraz wielkości wyświetlanego piksela obrazu. W ten sposób określa się ergonomiczną odległość obserwacji²⁴.

Typy operatorów

W zależności od wykazanych celów systemu stanowiska operatorów będą różniły się znacząco. Literatura wskazuje na dwa typy operatorów²⁵:

- Typ 1 – typowy monitoring, którego czynności polegają wyłącznie na obserwacji obrazów, sterowaniu kamerami i ich wyświetlaniem. Operator obserwuje obrazy do momentu wystąpienia czegoś nieoczekiwanego lub mieszczącego się w zakresie wcześniej zdefiniowanych zdarzeń w obrazie. Dokonuje na bieżąco analizy i reaguje. Typowe zadanie dozoru wizyjnego opisywane w literaturze, jako proces: obserwacja – detekcja – rozpoznanie – identyfikacja.
- Typ 2 – typowy kontroler procesu lub integracji systemów, który nie ma zadań monitoringu, a do dozoru wi-

zyjnego odwołuje się po uzyskaniu zewnętrznego bodźca np. sygnału alarmowego z innych systemów alarmowych (systemy zintegrowane) lub procesu przemysłowego (SCADA), może to być także informacja pozyskana przez telefon, radiotelefon itp.

Współczesne systemy ewoluują w kierunku połączenia zadań obu typów operatorów, jednak wymagania ergonomiczne i funkcjonalne dla jednego mogą nie być korzystne dla drugiego²⁶. Dodatkowo komplikuje to proces projektowania i funkcjonowania stanowiska. Badania autorów potwierdzają powyższe oraz pozwalają na wyróżnienie dwóch występujących powszechnie, charakterystycznych rozwiązań technicznych. Rozróżnienie związane jest z rodzajem stosowanych monitorów/ekranów – ściana monitorów a monitory stanowiskowe, będą to układy:

- Wertykalny – typ V – dla stanowisk wymagających wzmożonej, stałej obserwacji, rozpoznania zdarzeń, obiektów, funkcji prewencyjnego dozoru wizyjnego.
- Horyzontalny – typ H – dla stanowisk niewymagających wzmożonej, stałej obserwacji a jedynie ogólnego rozeznania i działania post incydentalnego, wymagającego sterowania systemami zintegrowanymi lub przemysłowymi (SCADA), występuje tu duża liczba obrazów z kamer, obiekt o dużej liczbie systemów elektronicznych, dużej skali integracji lub złożony proces przemysłowy.

Mogą wystąpić sytuacje, gdy stanowisko operatora będzie łączyło w sobie typy V i H, a także mieszane i powielone stanowiska z ustaloną hierarchią kompetencji operatorów ułożone w centrach operacyjnych²⁷.

Przykłady opisanych typów stanowisk operatorów systemu dozoru wizyjnego przedstawiają rysunki 3–5.

Przepisy i wytyczne niezbędne do przygotowania stanowiska operatora dozoru wizyjnego

Przygotowując stanowisko pracy operatora systemu dozoru wizyjnego, projektant ma do dyspozycji następujące wytyczne i zasady wiedzy technicznej:

²⁰ R. Pikaar, D. Lenior, K. Schreibers, D. Bruijn, *Human Factors Guidelines for CCTV system design*, Melbourne 2015.

²¹ J. Wood, R.N. Pikaar, E. Koningsveld, P. Settels, *CCTV Ergonomics: Case studies and practical guidance*, Amsterdam 2007.

²² PN-EN 62676-4: Systemy dozoru wizyjnego stosowane w zabezpieczeniach – Część 4: Wytyczne stosowania

²³ C. Mecwaldowski, R. Poklek, *Psychologiczne i techniczne aspekty stanowiska operatora dozoru wizyjnego. Część 2: Percepcja i uwaga w pracy obserwatora...* op. cit.

²⁴ Ibidem, s. 48.

²⁵ R. Pikaar, D. Lenior, K. Schreibers, D. Bruijn, *Human Factors ...* op. cit.

²⁶ Ibidem.

²⁷ C. Mecwaldowski, *Zarządzanie rozproszoną infrastrukturą krytyczną na przykładzie obiektów Służby Więziennej, „AS”*, 2019, nr 8.



Rys. 3. Przykład stanowiska H – horyzontalny
Źródło: Opracowanie własne na podstawie Winsted.



Rys. 4. Przykład stanowiska V – wertykalny
Źródło: Opracowanie własne na podstawie Winsted.



Rys. 5. Przykład wielostanowiskowego centrum operacyjnego
Źródło: Opracowanie własne na podstawie Winsted.

- Ustawa kodeks pracy z dnia 26 czerwca 1974 r. (tj. Dz. U. z 2019 r. poz. 1040) – BHP, Monitoring, obowiązki pracodawcy;
- Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U.1998.148.973);
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych;
- PN-EN ISO 11064: Ergonomiczne projektowanie centrów sterowania;
- PN-EN 50518: Centrum monitoringu i odbioru alarmu;
- PN-EN 62676: Systemy dozoru wizyjnego stosowane w zabezpieczeniach;
- PN-EN 9241: Ergonomia interakcji człowieka i systemu;

- PN-EN 50398: Systemy alarmowe – Systemy alarmowe łączone i zintegrowane;
 - PN-EN ISO/IEC 27000: Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji;
 - PN-ISO/IEC 29100: Technika informatyczna – Techniki bezpieczeństwa – Ramy prywatności;
 - PN-ISO 31000: Zarządzanie ryzykiem – Wytyczne;
 - Wytyczne budowy systemów dozoru wizyjnego np. stosowane w Wielkiej Brytanii, Stanach Zjednoczonych, Kanadzie;
 - Artykuły w czasopiśmie branżowych, rozwiązania producentów wyposażenia stanowisk operatorów, centrów dozoru, monitoringu, itp.
- Przygotowując stanowisko operatora dozoru wizyjnego należy rozpocząć od zastosowania zapisów ujętych w doku-

mencie „Wymagania użytkowe” systemu. Następnie należy zwrócić uwagę na następujące zagadnienia:

Zachowanie ergonomii stanowiska operatora:

- Wyposażenie w dedykowany, regulowany fotel obrotowy operatora (nie jest to biurowy fotel obrotowy);
- Dostosowana wysokość biurka, konsoli (powinna być regulowana w zależności od operatora, dostępne są meble z regulowaną wysokością łącznie z możliwością operacji w pozycji stojącej jak i siedzącej);
- Wyposażenie we wszystkie niezbędne urządzenia w odległości na wyciągnięcie ręki (klawiatura, manipulator, środki łączności itp. – jednocześnie minimalnej, niezbędnej ich liczby);
- Możliwość zmiany lokalizacji urządzeń na biurku dla praworęcznych;
- Maksymalna liczba obserwowanych scen/obrazów/monitorów wynikająca z przeprowadzonej analizy złożoności zadań, oczekiwanego czasu reakcji;
- Monitory szczegółowe pod kątem prostym względem oczu operatora, we właściwej odległości i wysokości (wyznaczone na podstawie norm);
- Maksymalny podział obrazu na cztery na monitorze szczegółowym (jeżeli jest to monitor panoramiczny (ang. *Ultra Wide*) należy stosować podział proporcjonalny do stanowiska wielomonitrowego);
- Monitory na ścianie, pod kątem prostym względem oczu operatora, we właściwej odległości i wysokości (wyznaczone na podstawie norm), nie

ICTProtegeGX.®

Jeden zintegrowany
system dla bezpieczeństwa
i automatyki obiektu.

- Kontrola Dostępu
- Dostęp mobilny (Bluetooth, NFC)
- System Sygnalizacji Włamania i Napadu
- Integracja z CCTV
- Rejestracja gości
- Zarządzanie windami
- Rejestracja Czasu Pracy
- Interkom (komunikacja SIP, VoIP)
- Automatyka Budynku
- Biometryka
- Integracja z dyspozytorami kluczy
- Integracja z zamkami do sejfów i ATM
- BacNET, Modbus

oraz szerokie możliwości integracji
z systemami zewnętrznymi

urmet
MIWI

Miwi Urmet Sp. z o.o.

91-341 Łódź,
ul. Pojezierska 90A
tel. 42 616 21 00
miwi@miwiurmet.pl

www.miwiurmet.pl

mogą być przestaniane przez stanowisko lub stanowiska;

- System musi umożliwiać szybkie przełączanie obrazów, szczególnie wybranego ze ściany monitorów na monitor szczegółowy-stanowiskowy.

Określenie uprawnień operatora w zakresie:

- Konfiguracji systemu i wykonywanych operacji;
- Dostępu do danych, w tym wykonywanie wydruków i kopii danych.

Wykonanie testów i kontroli (np. na podstawie załączników z przywołanych powyżej norm):

- Jakościowych systemu dozoru wizyjnego oraz innych systemów, których obsługa jest w zakresie zadań operatora;
- Realizacji zadań operatora zgodnie z procedurami i pomiarem czasu ich wykonania;
- Kontrole systemu, co 4 do 6 miesięcy weryfikujące zachowanie parametrów, konfiguracji systemu.

Szkolenia operatora:

- Stanowiskowe (obsługa techniczna w zakresie przydzielonych zadań, znajomość architektury obiektu i jego funkcjonowania, drogi ewakuacyjne, zasady łączności, rozpoznawanie założeń zdarzeń i reakcja zgodnie z przyjętymi założeniami w wymaganiach użytkowych), praca z asystą doświadczonego operatora;
- Specjalistyczne;
- Doskonalące (okresowe)²⁸.

Więcej informacji odnaleźć można w przywołanych powyżej normach, a także w artykułach dotyczących parametrów i ochrony centrum operacyjnego²⁹. Sto-

sowanie norm nie jest obowiązkowe, a to normy zawierają wymagania techniczne i użytkowe urządzeń, procedury badań, kolejność, wytyczne projektowania i eksploatacji systemów zabezpieczeń³⁰. Nie zwalnia to inwestora z obowiązku stosowania przepisów BHP i ergonomii. Autorzy uważają, iż wspomniane Rozporządzenie Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 r. powinno zostać zaktualizowane z nawiązaniem do norm, a zawarte w nim wytyczne uznane za obowiązkowe do stosowania w szerokim zakresie stanowisk pracy wyposażonych w monitory/ekrany. **Szczególnie, gdy norma (PN-EN ISO 11064-3) podaje definicję wskaźnika wizualnego łączącego definicję a dokładnie obejmującego wspólnym określeniem monitory, monitory ekranowe, monitory obrazowe, wyświetlacze itp.**

Obowiązujące rozporządzenie³¹ określa: wymagania BHP, ergonomię stanowiska i organizację pracy na stanowisku. Niestety, nieaktualizowane przez 21 lat, zawiera nieprzystające do współczesnych stanowisk pracy definicje związane z monitorami, ekranami, sprzętem komputerowym. Brak jednoznacznej wykładni prawa w tym zakresie, budzi kontrowersje i różne opinie, co do zakresu stosowania tego rozporządzenia³². Unikanie jego stosowania zdaniem autorów wynikało najczęściej, z zawartego w nim obowiązku dofinansowania zakupu okularów dla pracownika, jaki ciąży na pracodawcy. Specjaliści BHP, aby uniknąć zastosowania wytycznych rozporządzenia, chwyтали się wszelkich sposobów, aby nie uznać stanowiska pracy za stanowisko definiowane w ww. rozporządzeniu, a posługiwano się między innymi:

- Sztynną definicją monitora ekranowego, jako alfanumerycznego;
- Niewyposażaniem stanowiska w klawiaturę, drukarkę itp.;
- Montaż monitorów na ścianie poza biurkiem określanym, jako stanowisko;
- Kalkulacją czasu pracy, aby wypadało poniżej 4 godzin na dobę, itp.

Postępowano tak, mimo iż w 1999 roku w wyroku TSUE³³ do dyrektywy³⁴ sędzia rozszerzył definicję monitora ekranowego, o te wyświetlające grafikę i wideo, wskazał także na postępujący rozwój techniki i w związku z tym nie traktowanie tej definicji tak jednoznacznie³⁵. Obecnie należy ujednolicić definicję chociażby jak podaje wspomniana powyżej norma PN-EN ISO 11064-3 we **wskaźnik wizualny**.

Na występujące błędy, różne definicje i parametry w przepisach prawa od lat zwracają uwagę eksperci³⁶. Dotyczą one przede wszystkim niejednorodnego nazewnictwa, wskazania oczekiwań systemu bez precyzyjnego opisu, nie nadążających za rozwojem technologicznym aktualizacji prawa. Waldemar Więckowski w artykule³⁷ zauważa, że dozór nie jest równoznaczny z monitoringiem, a monitoring ma w swojej definicji określenie czynności, jako stałej. Ma to istotne znaczenie w kontekście wspomnianej powyżej odpowiedzialności dyscyplinarnej i karnej operatorów dozoru wizyjnego. ■

kpt. mgr inż. Cezary Mecwaldowski

Wykładowca zakładu szkolenia ochronnego w Centralnym Ośrodku Szkolenia Służby Więziennej w Kaliszu.

dr Robert Poklek

Psycholog, adiunkt na Wydziale Pedagogiczno-Artystycznym w Kaliszu Uniwersytetu im. Adama Mickiewicza w Poznaniu.

²⁸ C. Mecwaldowski, *Zasady doboru monitorowego – obserwatora w systemie monitoringu wizyjnego zakładu karnego*, [w:] *Możliwości i ograniczenia techniki w zastosowaniach penitencjarno-ochronnych. Humanistyczne i technologiczne wymiary systemu bezpieczeństwa*, (red.) R. Poklek, P. Dela, Euro-Media Sp. z o.o., Warszawa 2017, s. 51.

²⁹ Patrz: S. Parszowski, *Centrum operacyjne. Serce systemu bezpieczeństwa infrastruktury krytycznej*, „SEC&AS”, 2018, nr 5, s. 28; „SEC&AS”, *Planowanie i projektowanie centrum operacyjnego. Materiał powstał przy współpracy z Winsted*, „SEC&AS”, 2018, nr 5, s. 33; C. Mecwaldowski, R. Poklek, *Psychologiczne i techniczne aspekty stanowiska operatora dozoru wizyjnego. Część 1: Wrażenia i spostrzeganie...* op. cit., s. 47; C. Mecwaldowski, R. Poklek, *Psychologiczne i techniczne aspekty stanowiska operatora dozoru wizyjnego. Część 2: Percepcja i uwaga w pracy obserwatora...* op. cit., s. 46.

³⁰ S. Siudalski, *Stosowanie norm przy planowaniu ochrony – problemy*, „A&S”, 2018, nr 5.

³¹ Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz.U.1998.148.973).

³² J. Kowalski, *Monitor ochroniarza to nie monitor w biurze*, „ATEST”, 2005, nr 3.

³³ Wyrok Europejskiego Trybunału Sprawiedliwości C-11/99 (w sprawie Margarit Dietrich przeciwko Westdeutscher Rundfunk) ETS ustalił, że obejmuje to również monitory ekranowe przedstawiające nakręcone filmy w formie analogowej lub cyfrowej, w trybie prejudycjalnym podjął się interpretacji pojęcia „graficzny monitor ekranowy”

³⁴ Minimalne wymagania w dziedzinie bezpieczeństwa i ochrony zdrowia przy pracy z urządzeniami wyposażonymi w monitory ekranowe (piąta dyrektywa szczegółowa w rozumieniu art. 16 ust. 1 dyrektywy 87/391/EWG) (90/270/EWG) SEKCJA II OBOWIĄZKI PRACODAWCÓW Dz.UrzuEL.1990.156.14

³⁵ <https://www.rp.pl/artykul/706142-BHP---Monitory-ekranowe-Komentarz-do-rozporzadzenia-MPiPS.html>

³⁶ Patrz: W. Fiałka, *Jak wojewoda piksele liczył*, „Twierdza”, 2017, nr 2; S. Siudalski, *Normy obronne*, „A&S Polska”, 2018, nr 2

³⁷ W. Więckowski, *Kamera jaka jest, każdy widzi po swojemu*, „Systemy Alarmowe”, 2014, nr 2



securex[®]
P O L A N D
Międzynarodowe Targi Zabezpieczeń

ZAPRASZA
mtp
GRUPA

21-23.04.2020
POZNAŃ

www.securex.pl



Międzynarodowe
Targi Poznańskie



ZABEZPIECZ SWÓJ SUKCES!

W tym samym czasie

 **INSTALACJE**

 **EXPOPOWER**

 **greenPOWER**

 **SAWO**

 **POZNAŃ
DRONE
EXPO**

 **Poznań
Media Expo**

SLIM LINE – NOWE OBLCICZE DETEKCJI RUCHU



Z początkiem listopada oferta firmy SATEL została rozszerzona o nową serię czujek ruchu – SLIM LINE. Urządzenia te, oprócz wysokiej skuteczności w wykrywaniu ruchu w chronionym obszarze, oferują szereg dodatkowych, ciekawych rozwiązań.

Czujki z oznaczeniem PIR wyposażone są w pasywny czujnik podczerwieni. DUAL to modele dualne posiadające dodatkowo czujnik mikrofalowy. Wyjątkową cechą czujek LUNA jest funkcja oświetlenia. PRO spełniają wymagania normy EN 50131 dla Grade 3. Z kolei urządzenia z rozszerzeniem PET w nazwie, ignorują ruch niewielkich zwierząt domowych.

Wygląd

Każdy egzemplarz zamknięty jest w smukłej obudowie, charakteryzującej się lekkim designem. Dzięki temu wszystkie czujki ruchu pracujące w danym obiekcie, niezależnie od typu i oferowanych funkcji, mogą wyglądać tak samo. Utrudnia to intruzowi rozpoznanie modelu nadzorującego konkretne pomieszczenie. Ma także niebagatelny wpływ na estetykę instalacji alarmowej. Innym rozwiązaniem, podnoszącym atrakcyjność wizualną nowych urządzeń, jest możliwość wyboru koloru świecenia wskaźnika LED. W zależności od modelu urządzenia, dostępnych jest od czterech do nawet siedmiu różnych barw.

Skuteczna detekcja ruchu

Potężenie doświadczenia zdobytego przez lata produkcji czujek ruchu, z wykorzystaniem najnowszych technologii, zaowocowało opracowaniem nowego, za-

awansowanego algorytmu detekcji. Jest on dynamicznie dopasowywany do temperatury otoczenia, przez co jej zmiany nie mają wpływu na stabilność pracy czujek. Efektem jest niezawodne wykrywanie intruzów oraz ograniczenie występowania niepożądanych alarmów.

Czujki SLIM LINE wyposażone są w soczewki szerokokątne, zapewniające niezwykle skuteczną detekcję ruchu w obrębie całego nadzorowanego obszaru (o wymiarach nawet 20 m x 24 m). Opcjonalnie dostępne są wymienne fronty z soczewkami kurtynowymi lub dalekiego zasięgu – wymieniając cały element można szybko przystosować charakterystykę czujki np. do kształtu pomieszczenia. Wszystkie soczewki Fresnela stosowane w SLIM LINE zostały zaprojektowane i wyprodukowane w Japonii – specjalnie dla SATEL.

Dodatkowym atutem czujek LUNA i PRO jest funkcja kontroli strefy podejścia, czyli obszaru bezpośrednio pod urządzeniem. Można ją włączyć pokrętką umieszczoną od wewnętrznej strony frontu obudowy i w ten sposób zmienić położenie zintegrowanego uchylonego zwierciadła.

LUNA – czujki z funkcją oświetlenia

Modele LUNA posiadają wbudowany zestaw białych diod LED, załączanych zdalnie lub w reakcji na ruch w obszarze detekcji danej czujki. Urządzenia te znaj-

Rodzinę SLIM LINE tworzy dziesięć modeli:

SLIM-PIR	SLIM-DUAL
SLIM-PIR-PET	SLIM-DUAL-PET
SLIM-PIR-LUNA	SLIM-DUAL-LUNA
SLIM-PIR-LUNA-PET	SLIM-DUAL-LUNA-PET
SLIM-PIR-PRO	SLIM-DUAL-PRO



dą zastosowanie np. w korytarzach czy innych pomieszczeniach, gdzie do sprawnego i bezpiecznego przemieszczania się nie jest wymagane załączanie głównego oświetlenia. W urządzeniach tych programuje się dwa zestawy parametrów pracy (np. czułości czujników), między którymi można przełączać się zdalnie, podając masę na jeden z zacisków czujki. W jakim celu? Np. gdy strefa, do której przypisana jest czujka, czuwa – wykorzystywane są ustawienia eliminujące niepożądane alarmy. Natomiast, gdy czuwanie jest wyłączone, wbudowane diody oświetlające otoczenie czujki mogą włączać się w odpowiedzi na najdrobniejszy ruch.

Wersje PRO – czujki dla systemów Grade 3

Aktywny antymasking IR jest tym, co wyróżnia modele PRO. Wykrywają one próby zastąpienia soczewki polegające m.in. na jej zakryciu, zaklejeniu taśmą, zamalowaniu farbą lub bezbarwnym lakierem. Czujki te spełniają wymagania normy EN 50131 dla Grade 3 – można je stosować w obiektach szczególnie narażonych na włamanie. Mogą być dzięki temu częścią systemów nadzorujących banki, muzea, galerie sztuki, sklepy jubilerskie czy obiekty infrastruktury krytycznej. Tu warto dodać, że pozostałe przedstawicielki rodziny SLIM LINE spełniają wymagania dla Grade 2.

Szybki montaż, wygodna konfiguracja

Z myślą o ułatwieniu i przyspieszeniu pracy instalatorskiej, w czujkach SLIM LINE wprowadzono szereg ciekawych rozwiązań. Zaliczają się do nich m.in. wygodny mechanizm otwierająco/zamykający obudowy oraz zintegrowane rezystory 2EOL (1,1 k Ω , 4,7 k Ω i 5,6 k Ω w LUNA i PRO oraz 1,1 k Ω w pozostałych modelach).



LUNA i PRO wyposażone są w rozłączalną listwę zaciskową, umożliwiającą demontaż elektroniki bez odkręcania przewodów. Modele te wyróżnia też opcja zmiany za pomocą pilota ustawień takich jak: czułość czujników, tryb pracy czujki, sposób świecenia wskaźnika i oświetlenia LED. Konfiguracja może zatem odbywać się bez konieczności każdorazowego otwierania obudowy.

Autodiagnostyka czujek

Wszystkie urządzenia nowej serii zostały wyposażone w funkcję autodiagnostyki. W przypadku wykrycia nieprawidłowości w działaniu układu detekcji lub spadku napięcia poniżej 9 V na czas dłuższy niż 2 sekundy, czujka zgłosi awarię. Sygnalizacja takiej sytuacji polega na włączeniu przełącznika alarmowego i świeceniu wskaźnika LED.



DOPUSZCZENIE DO UŻYTKOWANIA WYROBÓW SŁUŻĄCYCH ZAPEWNIENIU BEZPIECZEŃSTWA PUBLICZNEGO LUB OCHRONIE ZDROWIA I ŻYCIA ORAZ MIENIA – ŚWIADECTWO DOPUSZCZENIA

Wprowadzenie

W poprzednich wydaniach czasopisma (nr 4/2019 i nr 5/2019) przedstawione zostały wymagania formalno-prawne w zakresie wprowadzania do obrotu wyrobów budowlanych stosowanych w ochronie przeciwpożarowej w oparciu o wymagania zharmonizowanych specyfikacji technicznych (tzw. certyfikacja europejska) lub krajowych specyfikacji technicznych (tzw. certyfikacja krajowa). Według autorów zaprezentowane artykuły stanowić mogą dobrą dawkę niezbędnej wiedzy dla osób zajmujących się tą tematyką w codziennej pracy. Podkreślenia wymaga również fakt, iż pewna grupa wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, wprowadzana do użytkowania w jednostkach ochrony przeciwpożarowej oraz wykorzystywana przez te jednostki do alarmowania o pożarze lub innym zagrożeniu oraz do prowadzenia działań ratowniczych, a także wyroby stanowiące podręczny sprzęt gaśniczy, może być stosowana wyłącznie po uprzednim uzyskaniu dopuszczenia do użytkowania. W niniejszym artykule autorzy omówią ten rodzaj atestacji.

Urządzenia przeciwpożarowe a wyroby podlegające dopuszczeniu do użytkowania

Przepisy prawne dotyczące ochrony przeciwpożarowej identyfikują pewną grupę urządzeń, zwaną urządzeniami przeciwpożarowymi, które bez wątpienia mają wpływ na szeroko pojęte bezpieczeństwo pożarowe, przede wszystkim umożliwiając przeprowadzenie skutecznej i bez-

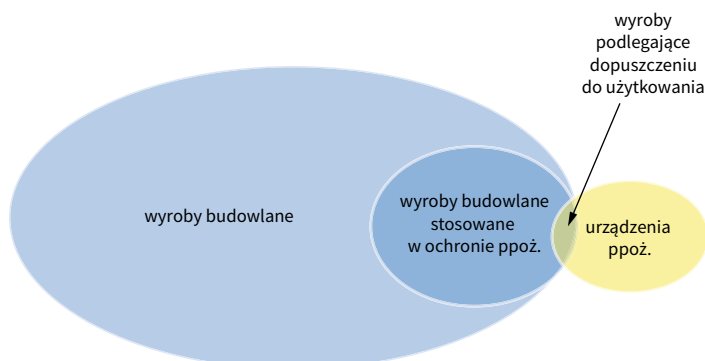
pieczonej ewakuacji ludzi w sytuacji zagrożenia oraz zwiększając bezpieczeństwo ekip ratowniczych podczas prowadzenia działań ratowniczo-gaśniczych. Wpływają zatem na bezpieczeństwo publiczne, poprzez ochronę zdrowia i życia ludzi użytkujących obiekty budowlane. Z uwagi na specyfikę ich działania i potrzebę wysokiej niezawodności pracy, wymagania techniczno-użytkowe stawiane tego typu urządzeniom są odpowiednio wyższe, niż te definiowane dla „zwykłych” urządzeń.

Większość z urządzeń przeciwpożarowych uznać można za wyroby o znaczeniu strategicznym w zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, które są wprowadzane do użytkowania w jednostkach ochrony przeciwpożarowej oraz wykorzystywane przez te jednostki do alarmowania o pożarze lub innym zagrożeniu, a także do prowadzenia działań ratowniczych (w tym również ewakuacyjnych).

Na podstawie upoważnienia ustawowego wynikającego z art. 7 ust. 14 ustawy z dnia 24 sierpnia 1991 r. o ochronie prze-

ciwpożarowej (Dz. U. 1991 Nr 81, poz. 351 z późn. zm.) [1] opublikowane zostało rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz. U. z 2007 r. Nr 143 poz. 1002) [2], które następnie zostało znowelizowane rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2010 r. (Dz. U. z 2010 nr 85 poz. 553) [3] oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2018 r. (Dz. U. z 2018 poz. 984) [4].

Dopuszczeniu do użytkowania podlega każdy kompletny wyrób wskazany w załączniku do rozporządzenia [2], znowelizowanego rozporządzeniami [3] i [4]. Łącznie jest to 89 rodzajów wyrobów, sklasyfikowanych w 15 grupach. Wśród nich wyróżnić można m.in.: elementy wyposażenia i środki ochrony indywidualnej strażaka, pompy, armaturę i osprzęt po-



Ryc. 1. Urządzenia przeciwpożarowe a wyroby podlegające dopuszczeniu do użytkowania
Źródło: opracowanie własne.

żarniczy, pojazdy pożarnicze, podręczny sprzęt gaśniczy, środki gaśnicze, elementy systemów alarmowania i powiadamiania, elementy systemów ostrzegania i ewakuacji, urządzenia do uruchamiania urządzeń przeciwpożarowych, znaki bezpieczeństwa i oświetlenie awaryjne oraz przewody i kable do urządzeń przeciwpożarowych

Jak wynika z analizy rozporządzenia [2] zmienionego rozporządzeniem [3] i [4], niektóre z wyrobów, które mogą być stosowane wyłącznie po uprzednim uzyskaniu dopuszczenia do użytkowania, to również wyroby budowlane (zgodnie z przepisami dot. wyrobów budowlanych) stosowane w ochronie przeciwpożarowej, które podlegają obowiązkowi wprowadzenia do obrotu (poprzedzonego przeprowadzeniem „europejskiej” lub krajowej oceny i weryfikacji stałości właściwości użytkowych). Przedmiotową sytuację zobrazowano na rycinie nr 1.

Wobec powyższego, w stosunku do części tych wyrobów ustawodawca wskazał potrzebę niezależnej atestacji, której celem jest potwierdzenie posiadania właściwości techniczno-użytkowych, niezbędnych do zapewnienia bezpieczeństwa publicznego lub ochrony zdrowia, życia oraz mienia.

Dopuszczenie wyrobów do użytkowania

Zasady wprowadzania wyrobów do użytkowania reguluje wspomniana już ustawa [1] wraz z aktami wykonawczymi, tj.:

- przywołanym powyżej rozporządzeniem [2], zmienionym rozporządzeniami [3] i [4], oraz
- *rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 czerwca 2007 r. w sprawie szczegółowych przepisów o dopuszczeniu wyrobów, opłat pobieranych przez jednostkę uprawnioną oraz sposobu ustalania wysokości opłat za te czynności (Dz. U. Nr 143, poz. 1001) [5].*

Dopuszczenia do użytkowania wyrobów wydawane są w formie świadectw dopuszczenia. Wydają je instytuty badawcze Państwowej Straży Pożarnej. Jednostką wskazaną do realizacji tego przepisu przez ministra właściwego do spraw wewnętrznych, zwaną dalej jednostką dopuszczającą, jest Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej – Państwowy Instytut Badawczy (CNBOP-PIB). Świadectwa dopuszczenia wyda-

wane są na czas określony, nie dłuższy niż 5 lat. W przypadku gdy technicznym dokumentem odniesienia, określonym w wymaganiach techniczno-użytkowych jest aprobaty techniczna (od 01.01.2017 r. zastąpiona przez krajową ocenę techniczną), dopuszczenia udziela się na okres zgodny z terminem ważności krajowej oceny technicznej.

Dopuszczenie może być wydane po stwierdzeniu:

- pozytywnej oceny właściwości użytkowych należycie zidentyfikowanego wyrobu, potwierdzonych, w zależności od potrzeb: badaniami, opiniami ekspertów lub innymi dokumentami, jeżeli wynika to z warunków stosowania wyrobu,
- pozytywnej oceny warunków techniczno-organizacyjnych (WTO) produkcji wyrobu.

Oceny właściwości użytkowych odpowiednio zidentyfikowanego wyrobu dokonuje się w oparciu o polskie normy, a w przypadku ich braku – wymagania techniczno-użytkowe, określone w przepisie [2] zmienionym przepisami [3] i [4].

W przypadku, gdy wyrób został:

- zgodnie z prawem wyprodukowany lub dopuszczony do obrotu w innym państwie członkowskim Unii Europejskiej albo w Republice Turcji,
- zgodnie z prawem wyprodukowany w innym państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) będącym stroną umowy o Europejskim Obszarze Gospodarczym,

dopuszczenie wydaje się po ustaleniu przez jednostkę dopuszczającą, że wyrób zapewnia bezpieczeństwo publiczne lub ochronę zdrowia i życia oraz mienia na poziomie nie niższym od określonego w polskich normach lub wymaganiach techniczno-użytkowych. Deklaracja o wprowadzeniu (wyprodukowaniu/dopuszczeniu) wyrobu, o którym mowa powyżej, nie jest podstawą do wydania świadectwa dopuszczenia do czasu ustalenia, że poziom bezpieczeństwa tego wyrobu nie jest niższy od określonego w polskich normach lub wymaganiach techniczno-użytkowych.

Proces dopuszczania wyrobów do użytkowania obejmuje następujące czynności:

- wstępną formalną ocenę wniosku o wydanie dopuszczenia oraz jego rejestrację,
- analizę wyników badań dostarczonych przez wnioskodawcę (tj. producenta wyrobu lub jego upoważnionego

przedstawiciela) i/lub przeprowadzenie badań próbek wyrobu przez jednostkę dopuszczającą,

- ocenę warunków techniczno-organizacyjnych produkcji wyrobu,
- analizę dokumentacji wyrobu oraz wydanie świadectwa dopuszczenia.

Wstępna formalna ocena wniosku o wydanie dopuszczenia oraz jego rejestracja

Proces dopuszczania rozpoczyna się od złożenia przez wnioskodawcę wniosku o przeprowadzenie dopuszczenia wyrobu do użytkowania, który dostępny jest do pobrania na stronie internetowej Instytutu. Wraz wnioskiem należy dostarczyć kompletną dokumentację (wskazaną w aplikacji), umożliwiającą m.in. dokładną identyfikację wyrobu i jego elementów składowych. Po otrzymaniu powyższych dokumentów jednostka dopuszczająca dokonuje ich wstępnej oceny. W przypadku otrzymania prawidłowo wypełnionego wniosku, wraz z kompletem niezbędnej dokumentacji, następuje jego rejestracja i tym samym formalne rozpoczęcie procesu dopuszczenia. Na tym etapie przekazywane jest wnioskodawcy potwierdzenie rejestracji wniosku, jak również program niezbędnych do wykonania badań laboratoryjnych. W przypadku negatywnego wyniku wstępnej oceny wniosku CNBOP-PIB informuje wnioskodawcę o konieczności dokonania niezbędnych poprawek, uzupełnień lub złożenia wyjaśnień.

Analiza wyników badań dostarczonych przez wnioskodawcę i/lub przeprowadzenie badań próbek wyrobu

Badania próbki/-ek wyrobu/-ów prowadzi laboratorium wskazane przez jednostkę dopuszczającą. W przypadku gdy wnioskodawca dostarczył wyniki badań laboratoryjnych na zgodność z mającym zastosowanie technicznym dokumentem odniesienia, jednostka dopuszczająca, uznaje wyniki badań uzyskane w laboratoriach akredytowanych (zgodnie z przepisami o systemie oceny zgodności), notyfikowanych lub zagranicznych (jeśli wynika to z umów międzynarodowych), o ile badania zostały wykonane metodami akceptowanymi przez CNBOP-PIB. Zakres badań wynika z technicznych dokumentów odniesienia, właściwych dla typu wyrobu, wymienionych w załączniku

do rozporządzenia [2], znowelizowanego rozporządzeniem [3] i [4].

Ocena warunków techniczno-organizacyjnych (WTO) produkcji wyrobu

Po otrzymaniu pozytywnych wyników badań laboratoryjnych jednostka dopuszczająca przeprowadza ocenę warunków techniczno-organizacyjnych produkcji wyrobu. Celem oceny WTO jest uzyskanie potwierdzenia w zakresie ustanowienia, wdrożenia i utrzymywania w miejscu/-ach produkcji wyrobu (zakładzie/-ach produkcyjnym/-ych) warunków techniczno-organizacyjnych, zapewniających stabilną i powtarzalną produkcję wyrobu spełniającego wymagania mających zastosowanie technicznych dokumentów odniesienia. Podczas oceny WTO zespół oceniający dokonuje analizy dokumentacji i oceny warunków wytwarzania oraz kontroli wyrobu. Zespół oceniający przedstawia wyniki oceny w raporcie/-ach z oceny WTO. Wymagania dotyczące warunków produkcji wyrobów określone zostały w dokumencie CNBOP-PIB pn. „Wymagania dotyczące warunków techniczno-organizacyjnych producenta wyrobów podlegających dopuszczeniu do użytkowania w ochronie przeciwpożarowej”, który dostępny jest na stronie internetowej Instytutu.

Analiza dokumentacji wyrobu oraz wydanie świadectwa dopuszczenia

Po uzyskaniu pozytywnego wyniku oceny WTO, jednostka dopuszczająca dokonuje analizy końcowej dokumentów zgromadzonych w procesie dopuszczenia, w tym przeprowadza ocenę:

- wyników badań wyrobu na zgodność z technicznym dokumentem odniesienia,
- wyników oceny WTO wykonanej w zakładzie/-ach produkcyjnym/-ych.

Na podstawie materiału zgromadzonego w procesie dopuszczenia podejmowana jest decyzja o wydaniu lub odmowie wydania dopuszczenia. W przypadku odmowy wydania dopuszczenia wnioskodawca otrzymuje na piśmie decyzję wraz z uzasadnieniem.

Potwierdzeniem udzielenia dopuszczenia jest wydane świadectwo dopuszczenia, które zawiera m.in.:

- numer świadectwa dopuszczenia,
- nazwę i adres wnioskodawcy (właściciela dopuszczenia),



Ryc. 2. Wzór świadectwa dopuszczenia wydawanego przez CNBOP-PIB
Źródło: opracowanie własne.

- nazwę i adres producenta,
- nazwę i adres zakładu/-ów produkującego/-ych wyrób,
- dane identyfikujące wyrób,
- stwierdzenie spełnienia wymagań określonych w polskich normach wyrobu lub wymagań techniczno-użytkowych,
- okres ważności świadectwa dopuszczenia.

Dopuszczenie wydawane jest oddzielnie dla każdego typu wyrobu, przy czym jednostka dopuszczająca może wydać dopuszczenie dla grupy odmian wyrobu, jeżeli wyniki badań próbek reprezentatywnych dla tej grupy wyrobów spełniają wymagania określone w wymaganiach techniczno-użytkowych lub w polskich normach wyrobu. Wartym zwrócenia uwagi jest fakt, iż dopuszczenie obejmuje wyroby wyprodukowane w okresie jego ważności.

Znakowanie dopuszczonego wyrobu

Posiadacz dopuszczenia powinien zapewnić, iż dopuszczony wyrób zostanie oznakowany znakiem jednostki dopuszczającej oraz dodatkowo numerem świadectwa dopuszczenia.

Znak jednostki dopuszczającej umieszcza się bezpośrednio na dopuszczonym wyrobie lub na etykiecie przymocowanej do niego w sposób widoczny, czytelny i niedający się usunąć. Jeżeli nie jest możliwe, ze względów technicznych, oznakowanie wyrobu w powyższy sposób,



umieszcza się je na opakowaniu jednostkowym lub opakowaniu zbiorczym wyrobu albo na dokumentach handlowych towarzyszących temu wyrobowi. Zaznaczyć należy przy tym, iż opisana powyżej sytuacja braku technicznej możliwości oznakowania dotyczy nielicznej grupy wyrobów. Zasady stosowania znaku jednostki dopuszczającej precyzuje dokument CNBOP-PIB pn. „Zasady postępowania się znakiem jednostki dopuszczającej CNBOP-PIB”, który jest dostępny na stronie internetowej Instytutu.

Kontrola świadectw dopuszczenia

Jednostka dopuszczająca prowadzi kontrolę dopuszczenia nie rzadziej niż raz w roku, w oparciu o roczny plan kontroli, a także doraźnie na podstawie informacji od użytkowników wskazujących na wady w dopuszczonym wyrobie. Kontrola dopuszczenia jest oceną zgodności wyrobu z wymaganiami technicznych dokumentów odniesienia i obejmuje następujące czynności:



Ryc. 3. Przykład oznakowania dopuszczonego wyrobu
Źródło: opracowanie własne.

- pobranie próbki wyrobu do badań,
- badanie próbki wyrobu,
- ocena zgodności wyrobu z wymaganiami technicznych dokumentów odniesienia na podstawie przeprowadzonych badań.

Po przeprowadzeniu kontroli, na podstawie protokołu z kontroli dopuszczenia podejmowana jest decyzja o utrzymaniu bądź cofnięciu dopuszczenia.

Dopuszczenie może być cofnięte nie tylko w wyniku negatywnego wyniku kontroli, ale również na wniosek jego posiadacza.

Zmiana zakresu dopuszczenia

Podkreślenia wymaga fakt, iż wszelkie zmiany materiałowe, konstrukcyjne lub technologiczne, mogące mieć wpływ na właściwości użytkowe dopuszczonego wyrobu lub na rozszerzenie zakresu jego stosowania, w okresie ważności dopuszczenia, mogą być dokonywane wyłącznie za zgodą jednostki dopuszczającej. W takim przypadku Instytut, na wniosek posiadacza dopuszczenia, przeprowadza proces zmiany dopuszczenia w zakresie stosownym do zgłoszonej zmiany.

W przypadku zmian w polskich normach oraz w wymaganiach techniczno-użytkowych, stanowiących podstawę udzielenia dopuszczenia jednostka dopuszczająca powiadamia posiadacza dopuszczenia o konieczności dostosowania wyrobu do obowiązujących (zmienionych) wymagań. W tym przypadku posiadacz dopuszczenia jest zobowiązany do przedstawienia dostosowanego wyrobu do badań w uzgodnionym terminie, lecz nieprzekraczającym 12 miesięcy.

Podsumowanie

Wyroby służące zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i 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 wyroby stanowiące podręczny sprzęt gaśniczy mają istotny wpływ na przeprowadzenie skutecznej i bezpiecznej ewakuacji ludzi w sytuacji zagrożenia oraz na zwiększenie bezpieczeństwa ekip ratowniczych podczas

prowadzenia działań ratowniczo-gaśniczych. Z tego powodu było i jest konieczne postawienie wymagań proporcjonalnych do celu – zapewnienie właściwego poziomu bezpieczeństwa pożarowego w obiektach budowlanych oraz właściwej ochrony ekip ratowniczych i osób zagrożonych. Należy zatem stwierdzić, iż wprowadzenie przez ustawodawcę, zgodnie z delegacją art. 7 ustawy [1], niezależnej atestacji dla określonej grupy wyrobów było i jest konieczne oraz uzasadnione. Zwrócenia uwagi wymaga również fakt zmieniających się potrzeb jednostek ochrony przeciwpożarowej, a także zauważalna dynamika definiowanych przez nie problemów w zakresie stosowania wyrobów na rzecz ochrony przeciwpożarowej. ■

Skład autorski:
Urszula Garlińska
Ilona Majka
Michał Pietrzak
Marcin Wawerek

Reklama

PARTNER sp. z o.o.

PRODUCENT
GŁOŚNIKÓW
DSO

Ważniejsze od ciszy...

www.part-ner.pl

Partner Sp. z o.o.
48-340 Głuchotądz
ul. Kopernika 1

Telefon:
(0048) 77 409 24 90
biuro@part-ner.pl

ŚWIADOMOŚĆ „ANTYTERRORYSTYCZNA” PRZEDSIĘBIORCÓW – CZĘŚĆ DRUGA

Wnikliwy czytelnik w części pierwszej tego artykułu odkrył albo upewnił się, że w 2016 roku ustanowiono z mocy Ustawy o działaniach antyterrorystycznych pewną pulę obowiązków, które należy realizować samemu. Tu należy dodać – realizować dla siebie, reprezentowanej przez siebie organizacji i tworzącego ją zespołu. Gdyby, zatem powtórzyć, litera art. 2 Ustawy określa podstawowe obszary działań antyterrorystycznych.

Zapobieganie zdarzeniom poprzez profilaktykę, w tym kształtowanie postaw, edukację i informację bieżącą, a także prewencję polegającą na przygotowaniu planu działania, wytworzeniu środowiska organizacyjnego do działania.

Przejmowanie kontroli nad zdarzeniami o charakterze terrorystycznym w drodze zaplanowanych przedsięwzięć. Zaplanowanych, a zatem nieukształtowanych pod wpływem przebiegu zdarzenia tylko wypracowanych na bazie analizy skutku działania sprawy.

Reagowanie, które podobnie jak przejmowanie kontroli budzi największe zdziwienie wśród osób wychowanych na zdewaluowanym i skompromitowanym sloganie „nic mi nie wolno, poza tym, co zlecą uprawnione służby”. Otóż tych „uprawnionych” najczęściej po prostu nie ma w pierwszej fazie zdarzenia. Oczywiście wyłączając działania wywiadowcze i obiekty lub zdarzenia o specjalnym statusie, np. chronione przez wzmocnione siły policyjne lub SOP. Pierwsze reakcje są, zatem zawsze po stronie zaatakowanego... i muszą pozostawać w zgodzie z prawem. Należy tu dodać aktualnym prawem, bo łatwo przeoczyć, że ustawa antyterrorystyczna zmieniła 32 inne ustawy.

I wreszcie usuwanie skutków, bo jak dotąd nawet największe w skali zdarzenia o charakterze terrorystycznym nie stały się kanwą apokalipsy. Przywrócenie zaś normalnego funkcjonowania może np. zatrzymać proces destabilizacji, o który zabiegają niektóre typy organizacji terrorystycznych lub ich mocodawcy.

Drażąc, zatem temat pozwolę sobie zwrócić uwagę czytelników na jeden,

wybrany subiektywnie akt wykonawczy, który jest istotnym przykładem logiki i semantyki regulacji ustawowej.

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP (Dz.U.2016 poz. 1101)

Ponieważ na analizę zasługuje każdy z punktów niniejszego Rozporządzenia, a możliwości wydawnicze ograniczają nieco treść, komentarzowi poddamy wyłącznie te punkty, które wymagają realizacji wewnątrz instytucji lub organizacji, czy przedsiębiorstwa. Co oznacza, że sformułowania „prowadzić przy użyciu Policji, Straży Granicznej lub Żandarmerii Wojskowej...” pominiemy pozostawiając w jak wierzę w dobrych rękach samorządu lub Wojewody. Na marginesie, przepisywanie literalnie takich punktów do planu działania, czy modułu zadaniowego np. przez kierownictwo spółki zarządzającej infrastrukturą krytyczną pod nazwą „zadania własne” (autor spotkał się osobiście z takim przykładem) jest nie tylko nieprawdziwe... jest śmieszne. Co innego, kiedy kierownictwo w ramach zadań własnych opisze tryb i formę współdziałania z takimi zadaniami służb mundurowych. Tym samym jednak optymalnie będzie czytać niniejszy komentarz z Rozporządzeniem otwartym w tle.

Rozporządzenie opisuje tryb i przedsięwzięcia towarzyszące kolejnym stopniom alarmowym Alfa – Bravo – Charlie – Delta oraz ich odpowiednikom CRP, czyli stopniom odnoszącym się do zagrożeń w cyberprzestrzeni. Właściwie sformułowanie „kolejnym” jest o tyle mylące, że ich ogłaszanie wcale nie musi stosować się do ich rosnącej kolejności. Może się, bowiem okazać, że okoliczności lub wiedza Agencji Bezpieczeństwa Wewnętrznego spowodują, iż pierwszym ogłoszonym stopniem będzie Delta, a przedsięwzięcia poprzedzających stopni należy „wykonać”. W tym przypadku ustawodawca nie przewidział określonego czasu na ich wykonanie, ale w ujęciu

praktycznym tryb „bez zbędnej zwłoki” będzie właściwy. Jeśli jest tu jakaś prawidłowość to z pewnością tą, że w związku z definicjami stopni można przewidywać, że stopnie Alfa i Bravo mogą częściej obowiązywać na dużym obszarze, np. kraju, a Charlie i Delta mogą dotyczyć nawet pojedynczego miasta lub obiektu. Najciekawszą lekturą może okazać się załącznik do rozporządzenia tj. **Szczegółowy zakres przedsięwzięć wykonywanych w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w poszczególnych stopniach alarmowych i stopniach alarmowych CRP**, który polecam lekturze każdemu, kto już dzisiaj odnajduje się w art. 4.1. Ustawy. Tym, którzy się nie odnajdują zwracam uwagę, że listę obiektów objętych obowiązkami może w zależności od potrzeb powiększyć Szef ABW. Warto też zauważyć, że pozostawianie bez możliwości uodpornienia na zdarzenia o charakterze terrorystycznym, na poziomie ukształtowanym przez otaczające nas środowisko, samo w sobie stanowi krytyczną podatność.

Alfa

... 2) prowadzić, w ramach realizacji zadań administratorów obiektów, wzmoczoną kontrolę obiektów użyteczności publicznej oraz innych obiektów, które potencjalnie mogą stać się celem zdarzenia o charakterze terrorystycznym; ...

Zwraca uwagę realizacja zadań administratorów obiektów. Rozporządzenie rzeczywiście dzieli środowisko na „obiekty”, co znajduje uzasadnienie zarówno w modus operandi sprawców, jak i możliwościach uodpornienia... obiektów właśnie. Warto jednak przypomnieć administratorom, że to oni, a nie „Pan z ochrony” są odpowiedzialni i żadna cesja nie pomoże na potrzebę przygotowania planu działania. Podstawową regulacją dającą się

w praktyce wykorzystać jest Regulamin obiektu, niekiedy zmieniony pod wpływem Antyterrorystycznego Planu Ochrony (jeśli jest wymagany).

... 3) zalecić podległemu personelowi informowanie odpowiednich służb w przypadku zauważenia: nieznanych pojazdów na terenie instytucji publicznych lub innych ważnych obiektów, porzuconych paczek i bagaży lub jakichkolwiek innych oznak nietypowej działalności; ...

Wydaje się proste i jasne. Nasz personel ma poinformować właściwe służby. W praktyce jednak warto rozważyć, kto konkretnie i kogo konkretnie ma informować. Czy i jak wykorzystać istniejącą hierarchię? Minimum trzy osobne procedury opisujące reakcje na pojazdy, porzucone paczki i bagaż oraz... jakiegokolwiek oznaki nietypowej działalności. Proste? No to proszę sobie wyobrazić ilość „nietypowych działalności” o których poinformuje „za plecami” administratora pracownik... Nie, nie ten bystry, ten z którego wszyscy się śmieją, bo wiezy w teorii spiskowe. Jednym słowem to zadanie dające pole do popisu na poziomie edukacji i katalogowania „nietypowych działalności”, które dla naszego konkretnego i specyficznego obiektu tworzą zagrożenie. Po co taka wysoka specyfikacja? Weźmy jako przykład 300 gramową puszkę pasztetu. Puszka z pasztetem w punkcie obsługi klienta jednego z samorządowych biur nie stanowi żadnego większego zagrożenia, ale ta sama puszka wniesiona na koncert, w dużej sali koncertowej ... rzucona z ostatniego rzędu ... może skrzywdzić, a nawet zabić. Jak nie energią kinetyczną to poprzez wywołaną panikę. I choć przykład przekoloryzowany – to wskazuje na konieczność – wygenerowaną potrzebą, a polegającą na wskazaniu obszaru lub charakteru takiej działalności.

... 10) dokonać przeglądu wszystkich procedur, rozkazów oraz zadań związanych z wprowadzeniem wyższych stopni alarmowych; ...

I stało się jasne, że od ogłoszenia pierwszego stopnia plan działania musi być opracowany do samego końca i bez miejsca na szukanie planowych rozwiązań i realizujących je osób w kolejnych etapach, a niekiedy również poparty inwestycjami w infrastrukturę.

Bravo

To stopień, który w opinii autora wprowadza najwięcej niestosowanych dotąd powszechnie rozwiązań i nowych obowiązków. Przy tym np. zarządcy szkół mogą dostrzec się wyraźnie w grupie realizującej konkretne i nietatwe w praktyce obowiązki.

... 5) ostrzec personel o możliwych formach zdarzenia o charakterze terrorystycznym; ...

Zwraca uwagę zwłaszcza przedmiot i podmiot ostrzeżenia. Ostrzegamy personel, a zatem mamy do czynienia z obowiązkiem administratora obiektu, który jest przez ten personel użytkowany. Nie zawsze tenże administrator jest jednocześnie pracodawcą i tu pole do przyszłych uzgodnień. Praktyka pokazuje, że stosunkowo najłatwiej jest to przeprowadzić w obiektach jednorodnych, np. administracji publicznej, gdzie zarządca jest często wyspecjalizowaną komórką tej samej organizacji. O wiele trudniej będzie np. w obiekcie, którego część pozostaje w użytkowaniu agentów. No i oczywisty problem generowany przez przestarzałe instrukcje – nie ostrzegamy o akcie terroru, zamachu, zagrożeniu ... ostrzeżenie dotyczy formy zdarzenia. Nowe formy semantyczne powodują zazwyczaj przejściowe problemy np. typologiczne. Proponuję obszary form podzielić na cztery główne obszary, w których relacja polega na tym, że priorytety naszych reakcji defensywnych różnią się, a niekiedy są nawet sprzeczne.

Oczywiście biegłe wytłumaczenie form wymaga odrobiny wysiłku intelektualnego i szkolenia, ale nawet amator zauważy, że dostępne instrukcje i rekomendowane zachowania w przypadku konkretnych działań sprawcy dają się kwantyfikować w ramach czterech wymienionych obszarów, a priorytety ... No cóż prosty przykład:



Źródło: wykład autorski Placówki edukacyjne w dobie terroryzmu, G. Cieślak, Collegium Civitas

W większości szkół jest jeden sygnał alarmowy – dzwonek modulowany. Jego etiologia, jako sygnału alarmowania pochodzi wprost z Ustawy o ochronie przeciwpożarowej z 1991 r. i trzeba przyznać w lwiej części działa wyśmienicie, zakładany jedynie przez siłę sprawczą w postaci czynnika ludzkiego. Co się dzieje według instrukcji przeciwpożarowej po ogłoszeniu sygnału? Uczniowie pod nadzorem nauczyciela i przy udziale osób funkcyjnych ewakuacji, udają się drogami ewakuacyjnymi do rejonu ewakuacyjnego. Tyle instrukcja, a w praktyce ... mniej uważny dydaktyk próbuje dogonić galopującą młodzież na korytarzu, ten bystrzejszy zrobił wcześniej „zaporę” w drzwiach i tonem nie znośącym sprzeciwu nakazał zmianę szyku z „roju” na „kolumnę” ... teraz z godnością wyprowadzi ich na korytarz i ... pogalopuje do rejonu ewakuacyjnego.

Czy nadaje się do użycia w przypadku formy zdarzenia terrorystycznego „zagrożenia w cyberprzestrzeni”? Nie bardzo. I nic nie szkodzi, bo całkowicie nie jest potrzebny. Podstawa reagowania w tej formie działania sprawcy to edukacja, świadomość zagrożeń i polityka bezpieczeństwa, która uwzględniła prawidłowe reakcje na incydent pojedynczego pracownika. Nie ma potrzeby wyjść na korytarz i dowiedzieć się, że w sali komputerowej na jednej jednostce PC odnotowano podejrzany mail.

Czy nadaje się na alarm bombowy? Wbrew pozorom tak. I w praktyce jest stosowany do takich zdarzeń, np. przy ewakuacjach towarzyszących powiadomieniom o podłożeniu ładunku. Choć wymaga wdrożenia jednej funkcjonalności. Otóż jeżeli to nie informacja i decyzja zarządcy (w tym przypadku dyrektora) jest powodem działania, a jest to przedmiot potencjalnie niebezpieczny to ujawniający go powinien zabezpieczyć miejsce znalezienia / ujawnienia. Jeżeli tego nie zrobi część ewakuujących może zmierzać w kierunku „do bomby”, bo tak każe” wykorzystywana droga ewakuacyjna. Sytuacja jest nie do przyjęcia, więc zabezpieczenie w praktyce polega na wyłączeniu pewnej części obiektu wraz z drogami ewakuacyjnymi. Nie da się tego zrobić np. oczekując na przybycie Policji i siłami jej funkcjonariuszy, bo po ogłoszeniu alarmu... uczniowie wyjdą na korytarz.

I teraz punkt kulminacyjny przykładu. Czy ten sam sygnał nadaje się na alarmowanie w przypadku formy zdarzenia – działania uzbrojonego sprawcy? Nie!



... 10) wprowadzić kontrolę wszystkich przesyłek pocztowych kierowanych do urzędu lub instytucji; ...

I żadna modyfikacja nie pomoże, bo każde wyjście na korytarz przysporzy większej ilości potencjalnych ofiar. W większości wykorzystanych scenariuszy, a autor przebadał około 50 w 200 placówkach szkolnych, nawet otwarcie drzwi klasy dla oceny sytuacji przez nauczyciela prowokowały sprawcę do wejścia do takiej klasy. Tu po prostu priorytetem jest coś dokładniej odwrotnego do ewakuacji – awaryjne zamknięcie, czyli lock’down. Sygnał zatem jest potrzebny, ale od początku sygnalizowania/alarmowania musi brzmieć inaczej, a instrukcje muszą opisywać inne zachowania.

Pozostał przykład skażeń i mowa tu o celowym działaniu na szkodę obiektu i użytkowników, a nie o np. katastrofie. Tu algorytm zbliżony do alarmu bombowego będzie miał zastosowanie, ale nie tyle zabezpieczenie rejonu, a izolacja czynnika skażenia będzie kluczowa. Inny sygnał? Jak najbardziej. I zupełnie inne kierunki ewakuacji lub jej całkowite zaniechanie.

Formy zdarzenia o charakterze terrorystycznym oraz metody ostrzegania o nich zasługują na oddzielny tekst, zależny zresztą od wyrażonej woli czytelników. Tymczasem wróćmy jednak do stopnia Bravo.

... 6) zapewnić dostępność w trybie alarmowym personelu wyznaczonego do wdrażania procedur działania na wypadek zdarzeń o charakterze terrorystycznym; ...

Jak widać personel funkcyjny będzie trzeba nie tylko wyłonić, ale i opracować system komunikacyjny, a w miarę potrzeb wprowadzić dyżury.

... 8) wprowadzić zakaz wstępu do przedszkoli, szkół i uczelni osobom postronnym; ...

To jedno z najtrudniejszych do praktycznej realizacji przedsięwzięć i jednocześnie w pełni uzasadnione. Trzeba jednak pamiętać, kto może w praktyce zarządzić taki zakaz. Wyłącznie dyrektor placówki lub rektor uczelni. Widać zatem rozszerzający sposób kwantyfikacji obowiązków wynikających z art. 2. Zwraca uwagę również bilans problemów technicznych i infrastrukturalnych. Identyfikacja tych „nie postronnych”, egzekwowanie zakazu, zabezpieczenie wejść nie używanych i nie obsadzonych przez personel, alarmowanie o naruszeniu zakazu, interwencje... Kilkadziesiąt konferencji, seminariów i spotkań oraz szkoleń uświadamiających z dyrektorami szkół uświadomiło autorowi, że trzy lata po uchwaleniu ustawy nikły odsetek szkół podjął działania skuteczne. Prawdę powiedziawszy również nikły podjął działania w ogóle.

I tu również nie łatwo o rozwiązania uniwersalne, choć najbliższe takiego stanu jest powołanie punktu kontroli przesyłki. Problem jednak z tym, że po zamknięciu biura podawczego w jednym z urzędów centralnych, w ramach ćwiczenia antyterrorystycznego, ok. 40% poczty i tak dotarło do obiektu. Problemem jest również obszar potencjalnych ryzyk, a zatem przesyłka z groźbą werbalną, urządzenie lub materiał wybuchowy i czynniki skażenia. „Bomba” to jurysdykcja Policji, a kolokwialnie opisywany „Wąglik” to Państwowa Straż Pożarna... z pomocą przychodzi regulacja Zarządzenia nr 36 KGP i zmiany w działaniu Państwowej Straży Pożarnej. Czemu zatem rekomenduję powołanie punktu kontroli. Po pierwsze, bo to my wyznaczmy miejsce, które sprawca może zaatakować. Jak wybierze sam to nie dziwny się, że okaże się nim być np. gabinet prezesa... w którym w przypadku zagrożenia skażeniem biologicznym Strażacy wyleją spore ilości płynu biobójczego. Brzmi źle, a jeszcze jak się dowiemy że to mądrzejsza nazwa wody z chlorem brzmi jeszcze gorzej. Żaden dokument, ani reprezentacyjny mebel nie będzie wyglądał już tak dostojnie, a wszystko przez to, że z koperty wysypało się trochę „mąki”. Po drugie zamiast szkolić każdego odbiorcę poczty wystarczy przeszkolić dwóch, trzech operatorów przesyłek. A przeszkolić trzeba. Po trzecie – to po prostu rozwiązanie sprawdzone „w boju” i pozwalające uniknąć niepożądanych i, o czym wiemy poskutkowo, niepotrzebnych ewakuacji, dekontaminacji, problemów. Problemów, które powstają nawet kiedy nikt nie ogłosił stopnia Bravo, ale ktoś tanim kosztem chciał sparaliżować funkcjonowanie organizacji.

Stopnie Charlie i Delta oraz CRP w części trzeciej

Grzegorz Cieślak

Ekspert profilaktyki i prewencji antyterrorystycznej Centrum Badań nad Ryzykami Społecznymi i Gospodarczymi Collegium Civitas. Wcześniej – członek rady programowej Centrum Badań nad Terroryzmem oraz Instytutu Analiz Informacji tej samej uczelni. Specjalista problematyki bliskowschodniej i Afryki północnej. Doradca ds. bezpieczeństwa w strategicznych obiektach infrastruktury krytycznej, transportowej, kultury i dziedzictwa narodowego oraz samorządu. Ekspert profilaktyki antyterrorystycznej, specjalista taktyki fizycznego zwalczania terroryzmu, uprawniony instruktor działań minersko – pirotechnicznych oraz Ekspert Ochrony Obiektów Dyplomatycznych z praktyką w krajach wysokiego ryzyka. Doświadczony specjalista w zakresie wdrożeń implikacji Ustawy o działaniach antyterrorystycznych. Autor projektów „(Nie)bezpieczna przesyłka”, „Strategia zabezpieczenia wielkopowierzchniowych obiektów komercyjnych”, „Tarcza”, „B.O.S.S.”, „BEHAV”, „Placówki edukacyjne w dobie zagrożeń terrorystycznych”, współautor metody szkoleń w zakresie prewencji antyterrorystycznej „LIDER” oraz „A.L.E.R.T.”. Autor metody szacowania ryzyka i oceny podatności dla obiektów administracji publicznej. Autor modelu zintegrowanego polityki bezpieczeństwa wraz modelem funkcjonalnym IT oraz koncepcji ochrony dla obiektów sieciowych. Współpracownik Centrum Prewencji Terrorystycznej ABW (TPCoE).

KOMPENDIUM WIEDZY SECURITY MANAGERA: BEZPIECZNY ŁAŃCUCH DOSTAW

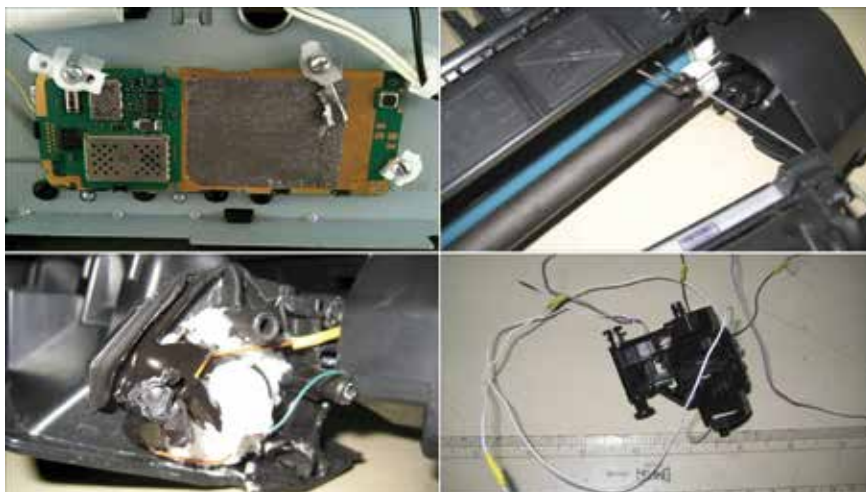
Od wielu lat lotnictwo cywilne, z oczywistych względów znajduje się w bezpośrednim zagrożeniu ze strony organizacji terrorystycznych. Jednym z powodów, dla których organizacje te decydują się atakować statki cywilne jest skala oddziaływania. Kilka set ofiar, nagłówki gazet, programy informacyjne odwołujące się do aktu terrorystycznego w telewizjach na całym świecie – efekt osiągnięty.

Organizacje terrorystyczne na świecie szukają jednak nowych celów ataków, by jeszcze bardziej wzmocnić poczucie zagrożenia i strachu. Szukają luk w systemie, które pozwolą skutecznie przeprowadzić akt bezprawnej ingerencji. O ile lotnictwo cywilne wykształciło dość skuteczne mechanizmy ochrony, uszczelniło system, o tyle doskonałym celem stał się rynek cargo lotniczego.

Niespełna dekada mija od najbardziej znanej próby popełnienia aktu bezprawnej ingerencji w historii rynku cargo lotniczego. W grudniu 2010 r. zostały ujawnione Improvised Explosive Devices (IED) ukryte w przesyłkach cargo nadanych z Jemenu na pokładach dwóch statków powietrznych, w związku z działaniami służb ochrony bazujących na podstawie informacji wywiadowczych.

Wydarzenie to pokazało, że nie tylko lotnictwo cywilne jest narażone na ataki terrorystyczne. Zapoczątkowało ono zarówno zmianę w podejściu Komisji Europejskiej do bezpiecznego łańcucha dostaw w zakresie cargo lotniczego, jak i też cargo transferowego.

Tematyka związana z bezpieczeństwem jest jedną z najważniejszych kwestii z zakresu funkcjonowania każdego rodzaju przedsiębiorstwa, niezależnie od branży i obszaru prowadzenia działalności. Jednocześnie samo pojęcie bezpieczeństwa w każdej organizacji może oznaczać zupełnie coś innego. Zdecydowana większość przedsiębiorstw ze względu na szeroko pojętą globalizację dostawców jest w dużym stopniu uzależniona od rozbudowanego łańcucha



Źródło: www.bbc.co.uk

dostaw, a zachowanie ciągłości ich działalności ma kluczowe znaczenie. Zagrożeniem więc jest niekontrolowane ich przerwanie. Transport cargo jest istotny dla przepływu towarów w krajowych i globalnych łańcuchach dostaw i dystrybucji. Od początku istnienia transport lotniczy specjalizuje się w przemieszczaniu drogą powietrzną wysokowartościowych w stosunku do wagi produktów, towarów łatwo psujących się, przesyłek wymagających szczególnego zabezpieczenia czy zwiększonej uwagi i w dostawach w sytuacjach awaryjnych dla nieprzewidzianych niedoborów. Wskaźnik produktów wysokowartościowych w stosunku do wagi odnosi się do względnie lekkich przesyłek, które generują wysokie koszty magazynowania w sytuacji wydłużającego się procesu transportowego. W przypadku towarów szybko psujących się opóźnienia czasowe w dostawie powodują znaczny spadek ich wartości. Z kolei brak krytycznych składników złożonych łańcuchów dostaw i dystrybucji oznacza długie i kosztowne przestoje całych procesów w przypadku niedostarczenia na czas brakujących elementów. Nowe branże, takie jak mikroelektronika czy branże zajmujące się wytwarzaniem farmaceutyków, części lotniczych lub wyrobów medycznych, w kategorii wartości przewozów stanowią

blisko trzy czwarte międzynarodowych ładunków lotniczych. Z danych ULC wynika, że tylko przez pierwsze trzy kwartały 2018 roku w polskich portach lotniczych obsłużono blisko 114 tys. ton towarów. Najwięcej, bo ponad 92,4 tys. ton, na Lotnisku Chopina w Warszawie. Rynek lotniczego cargo wzrósł w 2018 roku o 7,2%. Mając powyższe na uwadze, należy jednak przyjąć korektę, iż stanowi to jedynie 30% całego frachtu lotniczego, który faktycznie odlatuje z lotniska na terenie Polski. Pozostały towar trafia transportem drogowym do głównych portów lotniczych w Europie m.in. takich jak: Frankfurt, Amsterdam, Lipsk. Opublikowany w lutym 2018 r. przez IATA dokument „Air Cargo Strategy za jeden z priorytetów w branży określa „zwiększenie poziomu ochrony (Security) obok bezpieczeństwa (Safety)”.

Dla zrozumienia całego procesu bezpiecznego łańcucha dostaw i zagrożeń wobec których staje niezbędne jest poznanie ram prawnych, w których proces ten funkcjonuje.

Bezpieczny łańcuch dostaw oparty jest na trzech głównych aktorach, z których kluczową rolę odgrywa zarejestrowany agent.

Aneks 17 do konwencji o międzynarodowym lotnictwie cywilnym „Ochrona międzynarodowego lotnictwa cywilnego

przed aktami bezprawnej ingerencji” zobowiązuje „każde Umawiające się Państwo” do ustanowienia łańcucha dostaw w procesie ochrony, w którym zawiera się zatwierdzenie zarejestrowanych agentów i/lub znanych nadawców, jeżeli takie podmioty są zaangażowane we wdrażanie kontroli bezpieczeństwa lub innych środków kontroli w zakresie ochrony ładunków i poczty”

Zarejestrowanego agenta (ang. Regulated Agent) definiuje się jako „agenta, spedytora lub inny podmiot prowadzący działania biznesowe z operatorem, a także zapewniający środki kontroli w zakresie ochrony zaakceptowane lub wymagane przez odpowiednie władze w odniesieniu do ładunku lub poczty”. W ramach UE w dniu 29 kwietnia 2010 r. przyjęto rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 w sprawie wspólnych zasad ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 wraz z aktami wykonawczymi. Przepisy europejskie powielają terminologię zaproponowaną przez ICAO, jednocześnie doprecyzowując kwestie dotyczące obiegania się „przewoźnika lotniczego, agenta, spedytora lub innego podmiotu zapewniającego kontrolę w zakresie ochrony w odniesieniu do ładunku lub poczty” o status zarejestrowanego agenta. Zarejestrowany agent to podmiot, który poprzez zastosowanie środków kontroli w zakresie ochrony, m.in. kontrolę bezpieczeństwa nadaje status ochrony przesyłkom, dzięki czemu ładunki mogą w krótszym czasie trafić do magazynu linii lotniczej.

Środki kontroli w zakresie ochrony stosowane przez zarejestrowanego agenta obejmują dość szerokie spektrum. Kluczowym elementem zapewnienia bezpiecznego łańcucha dostaw dla zarejestrowanego agenta jest realizacja procesu sprawdzenia przeszłości osób zaangażowanych w stosowanie środków kontroli w zakresie ochrony jak też ich przeszkolenie z zakresu pkt 11.2.7 oraz 11.2.3.9. zał. do rozporządzenia wykonawczego KE nr 2015/1998.

Oczywiście poza przeszkolonym personelem oraz wyznaczeniem osoby odpowiedzialnej za ochronę (security manager), podmiot powinien posiadać odpowiednie zaplecze magazynowe, zabezpieczone w sposób zapewniający ochronę przesyłek cargo przed dostępem osób nieuprawnionych bądź bez nadzoru personelu zarejestrowanego agenta. Powyższe obejmuje wdrożenie systemu kontroli dostępu jak też skutecznego

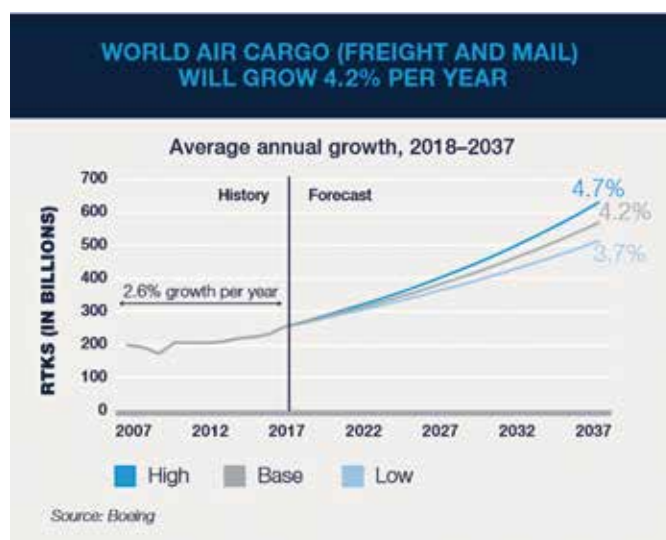
systemu sygnalizacji włamania i napadu. Oczywiście idealnym rozwiązaniem jest zapewnienie odseparowanej (wygrozionej) części magazynu dla składowania przesyłek cargo, które znajdują się w bezpiecznym łańcuchu dostaw. Rozwiązaniem alternatywnym, które również wypełnia wymogi narzucone przez ustawodawcę jest separacja ładunków z wykorzystaniem oznakowania poziomego oraz wsparta ewentualnym systemem detekcji ruchu. W tym miejscu warto podkreślić, iż posiadanie statusu zarejestrowanego agenta nie musi wiązać się zawsze z poniesieniem wysokich kosztów związanych z zakupem sprzętu ochrony wykorzystanego do kontroli bezpieczeństwa ładunków oraz nawiązaniem współpracy z przedsiębiorstwem posiadającym status SUFO (specjalistyczna umundurowana formacja obronna), które odpowiedzialne byłoby za fizyczne wykonywanie kontroli bezpieczeństwa w myśl wymogów określonych w Ustawie Prawo Lotnicze oraz Krajowym Programie Ochrony Lotnictwa Cywilnego. Zarejestrowany agent może bowiem zawrzeć odpowiednie porozumienia z innymi podmiotami, które posiadają już status zarejestrowanego agenta oraz odpowiednią infrastrukturę techniczną. Dzięki temu są w stanie zrealizować skuteczną kontrolę bezpieczeństwa lub też z racji stosowanego modelu biznesowego uczestniczyć jako ogniwo bezpiecznego łańcucha dostaw, którego zadaniem będzie nadanie statusu ochrony przesyłkom otrzymanym od podmiotów o statusie znanego nadawcy lub też zachowanie przedmiotowego łańcucha dla ładunków

otrzymanych od innych zarejestrowanych agentów.

Drugim podmiotem biorącym udział w procesie bezpiecznego łańcucha dostaw jest znany nadawca, który pełni kluczową rolę dla koncepcji obsługi ładunków.

Znany nadawca, podobnie jak zarejestrowany agent stosuje odpowiednie środki kontroli w zakresie ochrony oraz w analogiczny sposób jak zarejestrowany agent podlega wyznaczeniu realizowanemu przez Urząd Lotnictwa Cywilnego w oparciu o opracowany program ochrony dla danej lokalizacji, dla której obligatoryjne jest przeprowadzenie wizji lokalnej. Rola znanego nadawcy jest niezwykle istotna, gdyż de facto w jego lokalizacji następuje finalne zapakowanie przesyłki i sprawdzenie przez przeszkolony personel, czy stan ilościowy oraz jakościowy jest zgodny z procedowaną wysyłką. Znany nadawca poprzez odpowiedni opis procesu produkcyjnego w swoim programie ochrony zobowiązany jest do zdefiniowania, na którym etapie produkcji można stwierdzić, iż dany produkt można zidentyfikować jako identyfikowalny ładunek lotniczy. Od tego bowiem etapu należy wdrożyć odpowiednie środki kontroli w zakresie ochrony, które wyeliminują lub zminimalizują ryzyko nieuprawnionego dostępu do identyfikowalnego ładunku lotniczego.

Ponadto stosowanie przez znanego nadawcę zabezpieczenia finalnego produktu w postaci specjalnych taśm bądź numerowanych plomb czy też specjalnych opakowań umożliwiających łatwe stwierdzenie jego naruszenia także podlega wytycznym ustawodawcy. Powyższe



Fot. Średni w skali roku wzrost przewozu frachtu lotniczego w latach 2018–2037

Źródło: Boeing World Air Cargo Forecast.

sprowadza się do udowodnienia, iż Złoty Nadawca na każdym etapie produkcji bądź pakowania jest w stanie dokładnie wskazać odpowiedzialność za wystąpienie incydentu związanego z naruszeniem funkcjonującego systemu ochrony. W tym miejscu warto podkreślić, iż w dobie globalizacji wiele przedsiębiorstw stosuje jednakowe standardy w zakresie bezpieczeństwa i ochrony, co w praktyce sprowadza się do wdrożonego systemu ISO 28000 jak i też posiadania przez podmiot statusu upoważnionego przedsiębiorstwa AEO (ang. Authorised Economic Operator). Należy podkreślić, iż świadectwo AEO umożliwia podmiotom posiadającym ww. uprawnienia poddanie się płynnemu procesowi wyznaczenia jako złoty nadawca z racji wzajemnie uznawanych kryteriów i wymogów określonych w rozporządzeniu Parlamentu i Rady nr 300/2008 oraz rozporządzeniu wykonawczym KE nr 2015/1998.

Świadectwo AEO stanowi również bowiem gwarancję, że posiadająca go spółka cechuje się wysoką wiarygodnością wobec organów celnych. Uprawnienie promuje podmioty przestrzegające wymogów celnych i stosujące systemy zarządzania ewidencjami handlowymi i transportowymi pozwalające śledzić przepływ ładunków, co w znaczny sposób wpływa na poprawę jakości i bezpieczeństwa oraz ułatwia drogę do uzyskania statusu znanego nadawcy w bezpiecznym łańcuchu dostaw.

Mając na uwadze fakt, iż znaczna część cargo lotniczego obsługiwana jest transportem drogowym, a dopiero na kolejnym etapie trafia bezpośrednio do agenta handlingowego w danym porcie lotniczym, należy zwrócić szczególną uwagę na rolę przewoźnika drogowego w bezpiecznym łańcuchu dostaw. Przewoźnik drogowy jest ogniwem, który zapewnia płynny transport ładunków pomiędzy uczestnikami bezpiecznego łańcucha dostaw, ale i on musi spełnić odpowiednie wymogi prawne, aby zapewnić jego integralność. Przewoźnik drogowy zobowiązany jest do zapewnienia co najmniej szkoleń z zakresu ogólnej świadomości ochrony lotnictwa cywilnego, jak też sprawdzenia uczciwości swojego personelu, co de facto zgodnie z interpretacją Urzędu Lotnictwa Cywilnego sprowadza się do przeprowadzenia sprawdzenia przeszłości dla osób, które nie posiadają dostępu do strefy zastrzeżonej lotniska. Dokumentem, który powinien potwierdzić wdrożenie środków kontroli w zakresie ochrony przez przewoźnika drogowego jest deklaracja

przewoźnika stanowiąca dodatek 6-E do załącznika do rozporządzenia wykonawczego KE nr 2015/1998. Mając na uwadze aktualny trend uzyskiwania przez spedytorów/operatorów logistycznych statusu zarejestrowanego agenta na terenie Polski w głównej mierze w celu uczestniczenia oraz zachowania bezpiecznego łańcucha dostaw, przewoźnicy drogowi będący podwykonawcami ich zintegrowanych usług logistycznych oprócz wymogom jakościowym dot. posiadanej floty, jej dostępności oraz sprawności powinni podlegać także weryfikacji stosowania środków kontroli w zakresie ochrony przez swoich kontrahentów. Należy w tym miejscu podkreślić, iż to zarejestrowany agent, dla którego przewoźnik lotniczy wykonuje usługę transportową na podstawie odpowiednich umów handlowych odpowiedzialny jest w świetle przepisów o ochronie lotnictwa cywilnego za zachowanie integralności i bezpiecznego łańcucha dostaw. Praktyczny aspekt przedmiotowej weryfikacji z racji dużej fluktuacji kierowców oraz nowych firm transportowych rodzi coraz większe ryzyko, iż transport ładunków w bezpiecznym łańcuchu dostaw może być realizowany przez kierowców nie posiadających aktualnych szkoleń z zakresu ochrony lotnictwa cywilnego. To zjawisko może doprowadzić do stwierdzenia niezgodności przez audytorów krajowych ochrony lotnictwa cywilnego ULC i nałożenia kar finansowych w myśl postanowień Ustawy Prawo Lotnicze. Warto w tym miejscu zwrócić uwagę, iż obowiązująca legislacja wspólnotowa daje narzędzie do lepszego nadzoru nad działalnością przewoźników drogowych w sektorze bezpiecznego łańcucha dostaw, a mianowicie podmioty te mogą być uprawnione lub zatwierdzone przez właściwy organ danego Państwa Członkowskiego do świadczania usług transportowych dla ww. sektora.

Powyższą drogę wybrał niemiecki odpowiednik Urzędu Lotnictwa Cywilnego (LBA), który od marca 2017 r. wymaga, aby firmy transportowe zarejestrowane na terenie Republiki Federalnej Niemiec podlegały procesowi zatwierdzania po spełnieniu odpowiednich wymogów formalno-prawnych uwzględniających opracowanie programu ochrony. Wykaz zatwierdzonych przez LBA przewoźników drogowych zawiera już ponad 1300 podmiotów. Oczywiście taka forma nadzoru także może zostać uznana za prewencyjną, ale zdecydowanie ogranicza funkcjonowanie szarej strefy przewoźników drogowych ładunków lotniczych.

Ostatnim uczestnikiem bezpiecznego łańcucha dostaw jest podmiot o statusie znanego nadawcy, który do niedawna mógł być wyznaczany przez zarejestrowanego agenta tylko do transportu ładunków towarowymi statkami powietrznymi „cargo only”. Wraz z nowelizacją rozporządzenia wykonawczego KE nr 2015/1998 poprzez publikację rozporządzenia wykonawczego KE nr 2017/815 stwierdzono (na podstawie analiz ICAO), iż podmiot o statusie znanego nadawcy wyznaczony przez zarejestrowanego agenta stanowi potencjalne ryzyko dla zachowania odpowiedniego poziomu ochrony w ramach bezpiecznego łańcucha dostaw. Tym samym status wspomnianych podmiotów wygasa z dniem 30 czerwca 2021 r., zaś ich wyznaczanie od dnia 1 czerwca 2017 r. zostało wstrzymane.

Znając już praktycznie wszystkich uczestników bezpiecznego łańcucha dostaw warto zwrócić uwagę, iż wdrożenie wymogów z zakresu ochrony lotnictwa cywilnego w ramach procesu certyfikacji znanego nadawcy bądź zarejestrowanego agenta wymaga odpowiedniego doświadczenia oraz praktycznego aspektu funkcjonowania rynku cargo, jak też systemu ochrony lotnictwa cywilnego. Spedytorzy lub operatorzy logistyczni działają w otoczeniu biznesowym i posiadanie statusu zarejestrowanego wiąże się ściśle z podniesieniem konkurencyjności w branży logistycznej co sprowadza się do możliwości oferowania usług dopasowanych do potrzeb i wymogów swoich klientów. Główną zaletą uczestniczenia w bezpiecznym łańcuchu dostaw, niezależnie czy jako podmiot posiadający status znanego nadawcy bądź jego kontrahenta, czyli zarejestrowanego agenta jest skrócenie czasu obsługi terminalowej przesyłek w portach lotniczych na terenie polski oraz EU poprzez zwolnienie przesyłek cargo z kontroli bezpieczeństwa. Ponadto współpraca z zarejestrowanym agentem w ramach bezpiecznego łańcucha dostaw daje bardziej przejrzystą sferę opłat handlingowych poprzez możliwość zastosowania jednej stawki handlingowej. Posiadanie statusu zarejestrowanego agenta gwarantuje także mniejszą liczbę kontroli dokumentów i samych przesyłek. Z kolei w przypadku towarów podwyższonego ryzyka przedsiębiorstwo może skorzystać ze zwolnienia z obowiązku składania zabezpieczenia w określonych procedurach celnych. Wszystko to jest możliwe do skutecznego wdrożenia tylko, jeżeli zarejestrowany agent dostosuje

swoje procedury do środowiska biznesowego w jakim funkcjonuje jego klient, który także może być posiadaczem statusu znanego nadawcy. Proces pobierania ładunków od znanego nadawcy przez zarejestrowanego agenta uczestniczącego w bezpiecznym łańcuchu dostaw nie musi zawsze wiązać się z koniecznością nadawania statusu ochrony przesyłkom tylko i wyłącznie w lokalizacji zarejestrowanego agenta. Odpowiednio skonstruowane procedury wraz ze wskazaniem odpowiedzialności za ich realizację na każdym ich etapie, także przy uwzględnieniu stałej współpracy z operatorem logistycznym będącym równocześnie zarejestrowanym agentem, mogą zapewnić efektywny przepływ produktów finalnych w pełni zgodny z wymogami legislacji. Z racji kategorii towarów transportowanych drogą lotniczą, a w szczególności obejmujących produkty farmaceutyczne bądź elektronikę czy zaawansowane technologiczne podzespoły, konieczność przeprowadzenia skutecznej kontroli bezpieczeństwa, która często może wiązać się z koniecznością naruszenia opakowań produktów finalnych może wiązać się z nieprzewidywalnym wzrostem kosztów oraz czasu

na realizację ich dostawy do finalnego odbiorcy. Czy przedsiębiorstwa funkcjonujące na terenie Polski nie są świadome możliwych konsekwencji z tego wynikających? Porównując dane dot. liczby znanych nadawców wyznaczonych na terenie Niemiec, a ich liczbą na terenie Polski możemy zauważyć ogromną przepaść. Polscy przedsiębiorcy zdają się nie dostrzegać szans i możliwości, jakie daje im udział w bezpiecznym łańcuchu dostaw. Mając na uwadze obowiązujące przepisy znowelizowanej Ustawy Prawo Lotnicze, która nakłada kary finansowe na poziomie 30 tys. zł. w sytuacji ponownego stwierdzenia podczas kontroli sprawdzającej niewłaściwie zrealizowanej kontroli bezpieczeństwa ładunków i poczty, może się okazać, iż kolejny raz obsługa frachtu lotniczego napotka dodatkowe ograniczenia

związane z bardzo skrupulatnie prowadzoną kontrolą bezpieczeństwa. Wracając do kwestii właściwego poziomu ochrony dla przesyłek cargo warto zwrócić uwagę, iż bezpieczny łańcuch dostaw zapewnia identyfikowalność na każdym etapie tego procesu. Odróżnia go to od tradycyjnego modelu obsługi frachtu lotniczego. Ocze-kiwania środowiska biznesowego oraz rosnące wymagania klientów, oczekujących skrócenia czasów dostawy przesyłek do miejsca docelowego należy stwierdzić, iż bezpieczny łańcuch dostaw jest rozwiązaniem zapewniającym wyższy poziom bezpieczeństwa oraz lepszy standard jakościowy. Podstawowym wyzwaniem branży jest wzrost świadomości przedsiębiorstw na temat szans i możliwości, jakie proces ten ze sobą niesie. ■

Maciej Korczak

Absolwent: Politechniki Warszawskiej (Zarządzanie Produkcją), Szkoły Głównej Handlowej (Informatyczne systemy zarządzania), programu ICAO Aviation Security Professional Management Course – Concordia University – Montreal oraz programu audytorów ochrony lotnictwa cywilnego ECAC. Audytor Wiodący ISO 9001. Wewnętrzny Audytor Ochrony lotnictwa Cywilnego – Instruktor. Od 16 lat związany zawodowo z branżą lotniczą. Kierownik w centrum Operacyjnym przewoźnika lotniczego – Security Manager. Specjalista ds. bezpieczeństwa Urzędu Lotnictwa Cywilnego. Konsultant z zakresu bezpiecznego łańcucha dostaw ładunków i poczty. Uczestnik wielu projektów z zakresu modernizacji infrastruktury lotniskowej w tym systemu bezpieczeństwa jak i też międzynarodowych wydarzeń/konferencji z zakresu lotnictwa. Praktyk.

Reklama

PRENUMERATA 2020!

Zamów prenumeratę czasopisma Ochrona i Bezpieczeństwo na 2020 rok a otrzymasz 2 WYDANIA GRATIS! **

START ZA DARMO!*



60 zł

NOWA NAZWA I LOGO OD NR 1/2020

* Oferta dla nowych prenumeratorów

** Wydania gratisowe Ochrony Mienia i Informacji nr 5/2019 i 6/2019



prenumerata@mediafachowe.pl



22 535 32 29



www.czasopismo.net

ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA – JEDEN Z FILARÓW BEZPIECZEŃSTWA ORGANIZACJI

Każdy podmiot działający na rynku, niezależnie od rodzaju, wielkości, przynależności do danego sektora lub gałęzi gospodarki, formy własności czy pełnionej roli stale narażony jest na różnego typu „incydenty”, które mogą zakłócić lub nawet przerwać jego działalność operacyjną. Wachlarz tych zdarzeń jest szeroki – mogą to być sytuacje ekstremalne takie jak klęski żywiołowe, ale częściej jest to coś bardziej powszechnego i prawdopodobnego jak zanik zasilania czy pęknięta rura wodociągowa lub awaria serwera. Każda taka awaria to zakłócenie zdolności organizacji do wykonywania jej normalnych działań co w konsekwencji może wpłynąć na klientów i interesariuszy powodując dodatkowe koszty i tworząc potencjał strat finansowych i niefinansowych.

Na przestrzeni ostatnich kilkunastu lat Zarządzanie Ciągłością Działania (eng. business continuity management – BCM) rozwinęło się z ledwie tolerowanego dodatku do potężnego narzędzia pomagającego organizacjom nie tylko skutecznie reagować i zarządzać szkodliwym incydem, ale także zabezpieczyć i aktywnie chronić je przed ich skutkami. Obecnie można obserwować dalszą ewolucję czyniącą z Zarządzania Ciągłością Działania zasadniczy fundament procesu kompleksowego i spójnego zarządzania ryzykiem i bezpieczeństwem – czyli tzw. budowanie odporności organizacji.

W przypadku większości organizacji proces zarządzania ciągłością działania obejmuje planowanie, nadzór i realizację działań w zakresie: zarządzania kryzysowego; odtwarzania procesów, infrastruktury i zasobów niezbędnych do wznowienia działalności operacyjnej; usunięcia skutków awarii; planowania awaryjnego i powrotu do normalnej działalności biznesowej.

Dzięki wdrożeniu zarządzania ciągłością działania organizacje są znacznie lepiej przygotowane do przewidywania, zapobiegania i reagowania na incydenty, które mogą zakłócić jej funkcjonowanie

a tym samym skutecznie zmniejszyć lub niekiedy nawet wyeliminować koszty i potencjalne straty spowodowane incydem.

Zarządzanie ciągłością działania to nie tylko propozycja dla dużych korporacji czy sektora publicznego (infrastruktury krytycznej, operatorów usług kluczowych). Zasady Zarządzania Ciągłością Działania mają zastosowanie do wszystkich organizacji, bez względu na wielkość czy profil prowadzonej działalności. W rzeczywistości sprawne Zarządzanie Ciągłością Działania może przynieść znaczące korzyści mniejszym firmom umożliwiając im budowanie przewagi nad konkurencją, poprawę (poprzez kompleksowe oddziaływanie na każdej płaszczyźnie) bezpieczeństwa i zarządzania ryzykiem czy ochronę interesów klientów i właścicieli.

Mimo, iż początki zarządzania ciągłością działania sięgają lat 60 i 70 XX w., to gwałtowny rozwój nastąpił dopiero w drugiej połowie lat 90 poprzedniego stulecia. Pierwszą próbą zmierzenia się z tym zagadnieniem poprzez opracowanie standardu, który mógłby być wykorzystywany przez różne organizacje, było wydanie przez Disaster Recovery Institute International w 1997 r. „Zasad Zawodowych dla Specjalistów w Zakresie Planowania Ciągłości Działania”. Następnie w roku 2000 Business Continuity Institute wydało „Dobre Praktyki”, będące podstawą do opracowania nowego standardu dotyczącego ciągłości działania (PAS 56 „Guide To Business Continuity Management”) oraz ciągłości świadczenia usług informatycznych (PAS 77 „IT Service Continuity Management. Code of Practice”). Prawdziwa rewolucja zaszła w roku 2007 gdy PAS 56 został zastąpiony przez Brytyjski Standard BS 25999 (Business Continuity Management) – był to pierwszy, prawdziwie uniwersalny standard który można było wdrożyć i certyfikować w dowolnej organizacji.

W roku 2012 w oparciu o BS25999 zostaje wydana międzynarodowa norma ISO 22301, która jest de facto lekko zmo-

dyfikowanym standardem brytyjskim. Ostatnim „kamieniem milowym” zarządzania ciągłością działania ujętym w normę jest ISO 22316 z roku 2018, w której to Zarządzanie Ciągłością Działania z jednym z elementów zintegrowanego zarządzania organizacją staje się fundamentem strategicznego i operacyjnego procesu budowania odporności organizacji (synergia zarządzania ciągłością działania, zarządzania ryzykiem oraz zarządzania bezpieczeństwem i jakością).

W Polsce proces zarządzania ciągłością działania pojawił się dopiero na przełomie wieków, a pierwszym poważnym problemem z jakim musiały sobie poradzić organizacje i specjaliści od BCM był problem roku 2000 w systemach IT. Początkowo zarządzanie ciągłością działania koncentrowało się na problemach związanych z odtwarzaniem danych i infrastruktury IT, czyli działaniami z obszaru „disaster recovery”. Dopiero po ataku na WTC we wrześniu 2011 roku zaczęto rozszerzać Zarządzanie Ciągłością Działania także na obszary ogólnobiznesowe. Pierwsze regulacje w ramach Ustaw sektorowych pojawiają się w drugiej połowie lat 90 (Ustawa, Prawo bankowe; Ustawa, Prawo energetyczne; Ustawa o systemie ubezpieczeń społecznych).

Obecnie (oprócz norm ISO) w Polsce zarządzanie ciągłością działania jest także standardem wymaganym przez regulatora pośrednio lub bezpośrednio poprzez następujące akty prawne:

- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. Nr 89, poz. 590, z późn. zm.)
- Załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej – „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje” (Narodowy Program Ochrony Infrastruktury Krytycznej – Uchwała nr 121/2018 Rady Ministrów),
- Ustawa o krajowym systemie cyberbezpieczeństwa – z dnia 5 lipca 2018 r. (Dz.U. 2018 poz. 1560)

- Ustawa, Prawo bankowe – z dnia 29 sierpnia 1997 (Dz.U. z 2002 r. nr 72, poz. 665, z późn. zm.)
- Urząd Komisji Nadzoru Finansowego – Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach (Rekomendacja 11)
- Urząd Komisji Nadzoru Finansowego – Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Rekomendacja 15)
- Ustawa, Prawo komunikacyjne – z dnia 16 lipca 2004 r. (Dz.U. z 2004 r. nr 171, poz. 1800, z późn. zm.)
- Ustawa, Prawo energetyczne – z dnia 10 kwietnia 1997 r. (Dz.U. z 2006 r. nr 89, poz. 625, z późn. zm.)
- Ustawa, Prawo pocztowe – z dnia 12 czerwca 2003 r. (Dz.U. z 2008 r. nr 189, poz. 1159, z późn. zm.)
- Ustawa o systemie ubezpieczeń społecznych – z dnia 13 października 1998 r. (Dz.U. z 2009 r. nr 205, poz. 1585, z późn. zm.)

Aby wdrożyć skuteczny proces zarządzania ciągłością działania nie wystarczy znajomość norm i dobrych praktyk, przede wszystkim ważne jest aby Zarządzanie Ciągłością Działania zostało włączone w kulturę organizacji jako jej stały i nieodłączny element. Tego nie da się zrobić bez pełnego i świadomego zaangażowania kierownictwa organizacji poczynając od zarządu a skończywszy na kierownikach jednostek realizujących krytyczne procesy biznesowe. Jeśli wielkość organizacji na to pozwala dobrym rozwiązaniem zapewniającym ciągłość inicjatywy i możliwość przewyższania trudności jakie zwykle towarzyszą wdrożeniu Zarządzania Ciągłością Działania jest powołanie dedykowanego Komitetu (w skład którego wejdzie min. jeden członek zarządu wyznaczony na gestora procesu). W mniejszych organizacjach rolę gestora powierza się osobie z najwyższego kierownictwa, zaś sam BCM umieszcza się tak aby podlegał bezpośrednio pod gestora.

Kluczową osobą dla procesu jest tzw. BCM Manager – powinna to być osoba raportująca bezpośrednio do najwyższego kierownictwa (zarząd, gestor). Ideальnym kandydatem jest osoba posiadająca szeroką wiedzę dotyczącą struktury biznesowej organizacji, procesów i ludzi. Pożądane jest aby posiadała umiejętności komunikacyjne i interpersonalne oraz umiała dobrze zarządzać zespołem i/lub projektem.

Aby móc w pełni korzystać z profitów zarządzania ciągłością działania poniższe warunki muszą zostać spełnione:

- Zarządzanie Ciągłością Działania jest integralną częścią ładu korporacyjnego
- Działania w ramach Zarządzania Ciągłością Działania muszą być zgodne, koncentrować się i bezpośrednio wspierać strategię i cele biznesowe organizacji
- Zarządzanie Ciągłością Działania musi zapewniać odporność biznesową w celu optymalizacji dostępności produktów i usług organizacji
- Zarządzanie Ciągłością Działania musi być optymalizowane pod kątem efektywności kosztowej
- Zarządzanie Ciągłością Działania musi być wdrożony w organizacji świadomie jako wartość dodana podnosząca bezpieczeństwo, elastyczność i efektywność biznesową a nie tylko ze względu na wymagania prawne i regulacyjne.

Wdrażając proces zarządzania ciągłością działania należy wykonać pięć kroków (które należy powtarzać po każdym pełnym przejściu cyklu):

1. Przeanalizuj swoją firmę
2. Oceń ryzyko
3. Opracuj strategię
4. Opracuj swój plan ciągłości działania
5. Przetestuj plan ciągłości działania

Przeanalizuj swoją firmę – innymi słowy dowiedz się co jest dla niej kluczowe (produkty, usługi, procesy, obszary, dostawcy, etc...) i na jakie zagrożenia i ryzyka jest narażona. Na tym etapie zazwyczaj umiejscawia się proces i strukturę Zarządzania Ciągłością Działania w szkielecie organizacji.

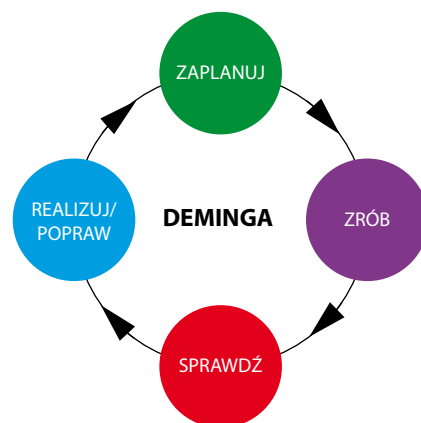
Oceń ryzyko – czyli sprawdź co może zakłócić lub przerwać działalność organizacji, ustal jakie jest prawdopodobieństwo wystąpienia takiego zdarzenia,

oszacuj jakie to może mieć skutki (zarówno finansowe jak i niefinansowe) oraz zweryfikuj jak bardzo na dane ryzyko jest podatna organizacja i czy dysponuje już jakimiś mechanizmami mitygującymi lub kompensującymi dane ryzyko.

Opracuj strategię – w oparciu o ocenę ryzyka, podatności i istniejące działania mitygujące określ pryncypia i sposób postępowania w przypadku materializacji ryzyka.

Opracuj swój plan – czyli sformalizuj i opisz co, jak, kiedy i kto będzie robić aby przyjęta strategia postępowania mogła zostać rzeczywiście zrealizowana zgodnie z przyjętymi założeniami.

Przetestuj plan – czyli sprawdź empirycznie, czy opracowany plan można zrealizować, czy efekty jego realizacji spełnią oczekiwania organizacji oraz czy występują elementy wymagające poprawy/korekty.



Ze względu na szybko zmieniający się charakter warunków biznesowych proces Zarządzania Ciągłością Działania nie jest procesem statycznym ale cyklicznym. Podobnie jak inne systemy jakościowo-zarządcze Zarządzanie Ciągłością Działania jest procesem samodoskonalącym się, funkcjonującym w oparciu o cykl (koło). ■

Hubert Łabęcki

Ekspert w zakresie zarządzania kryzysowego i zarządzania ciągłością działania, Audytor Wiodący BS25999 oraz ISO/IEC27001 (IRCA), Risk Manager ISO31000. Absolwent Wydziału Zarządzania i Informatyki Zachodniopomorskiej Szkoły Biznesu. Trener, prelegent i uczestnik licznych szkoleń i konferencji poświęconych zarządzaniu ryzykiem, bezpieczeństwu informacji i zarządzaniu ciągłością działania.

Od niemal 20 lat zawodowo zajmuje się problematyką zarządzania ciągłością działania w sektorze finansowym i administracji publicznej. Doświadczenie zawodowe zdobył wdrażając standardy i zarządzając procesem ciągłości działania i zarządzania kryzysowego w czołowych instytucjach sektora finansowego (m.in. Grupa Citi, Bank BGŻ, Polbank EFG, Grupa Raiffeisen A.G) oraz usług IT&N dla sektora publicznego. Prowadził liczne i różnicowane audyty zgodności w zakresie bezpieczeństwa informacji i ciągłości działania oraz kierował projektami przygotowania i wdrożenia systemu BCM w instytucjach finansowych krajowych i zagranicznych.

Obecnie związany zawodowo z Grupą Kapitałową BNP. Przewodniczący Grupy ds. Ciągłości Działania przy Związku Banków Polskich. Za wkład w budowę bezpieczeństwa sektora finansowego odznaczony w roku 2016 przez Związek Banków Polskich „Medalem im. Mikołaja Kopernika”.

MAXPRO® CLOUD

BEZPIECZEŃSTWO W CHMURZE



MAXPRO® Cloud

Zintegrowane systemy zabezpieczeń w chmurze MAXPRO® Cloud. Idealne rozwiązanie szczególnie dla małych i średnich obiektów, umożliwiające właścicielom firm zarządzanie bezpieczeństwem pojedynczych lub wielu lokalizacji jednocześnie. Jest to zintegrowany, oparty na chmurze system zarządzania telewizją dozorową, kontrolą dostępu oraz sygnalizacją włamania i napadu. Zabezpieczenia w chmurze to zwiększona wydajność, bezpieczeństwo, efektywność dla biznesu i wygoda użytkowania.

Nowy wymiar bezpieczeństwa!

Poproś o bezpłatną wersję DEMO już dziś przez stronę maxprocloud.com/ee

Honeywell | THE FUTURE IS WHAT WE MAKE IT

Wysokiej klasy platforma Microsoft Azure



TAP - Systemy Alarmowe Sp. z o.o., ul.
Tatrzańska 8, 60-413 Poznań
e-mail: tap@tap.com.pl, www.tap.com.pl

© 2019 Honeywell International. Wszelkie prawa zastrzeżone

MAXPRO® CLOUD

– USŁUGI HOSTINGOWE W CHMURZE

MAXPRO® Cloud firmy Honeywell jest w pełni zintegrowaną platformą umożliwiającą połączenie do chmury systemów sygnalizacji włamania i napadu, kontroli dostępu oraz telewizji dozorowej lub kombinacji tych systemów.

Zaprojektowana przez Honeywell i obsługiwana przez Microsoft Azure, MAXPRO Cloud łączy wiodącą w branży wiedzę na temat systemów bezpieczeństwa z najlepszą w swojej klasie technologią chmurową.

Jest to rozwiązanie idealne dla małych i średnich przedsiębiorstw, które zapewnia szybką i dostosowaną do potrzeb obsługę systemu bezpieczeństwa w jednym lub większej liczbie budynków. Użytkownik może zarządzać systemem bezpieczeństwa z dowolnego miejsca i w dowolnym momencie, za pomocą standardowej przeglądarki internetowej lub innowacyjnej aplikacji mobilnej.

Zdalna konfiguracja oraz zarządzanie poszczególnymi obiektami, urządzeniami, harmonogramami i użytkownikami zapewniają obniżenie kosztów eksploatacji i większą wydajność w przypadku obsługi wielu instalacji.

W skład szerokiej gamy obsługiwanych przez MAXPRO Cloud systemów wchodzi obecnie systemy sygnalizacji włamania i napadu Galaxy Dimension, Galaxy Flex+, Galaxy Flex oraz Vista, syste-

my kontroli dostępu NetAXS, rejestratory sieciowe NVR (HEN) oraz rejestratory cyfrowe DVR (HQA).

Od stycznia 2020 roku gama ta zostanie rozszerzona o nowe systemy sygnalizacji włamania i napadu Maxpro Intrusion oraz systemy kontroli dostępu Maxpro Access.

MAXPRO Cloud zapewnia podłączenie typu „plug and play” oraz automatyczne dodanie systemu do chmury z wykorzystaniem protokołu ISOM, wyłącznie na podstawie MAC adresu kontrolera, bez otwierania portów, co powoduje znaczne zwiększenie

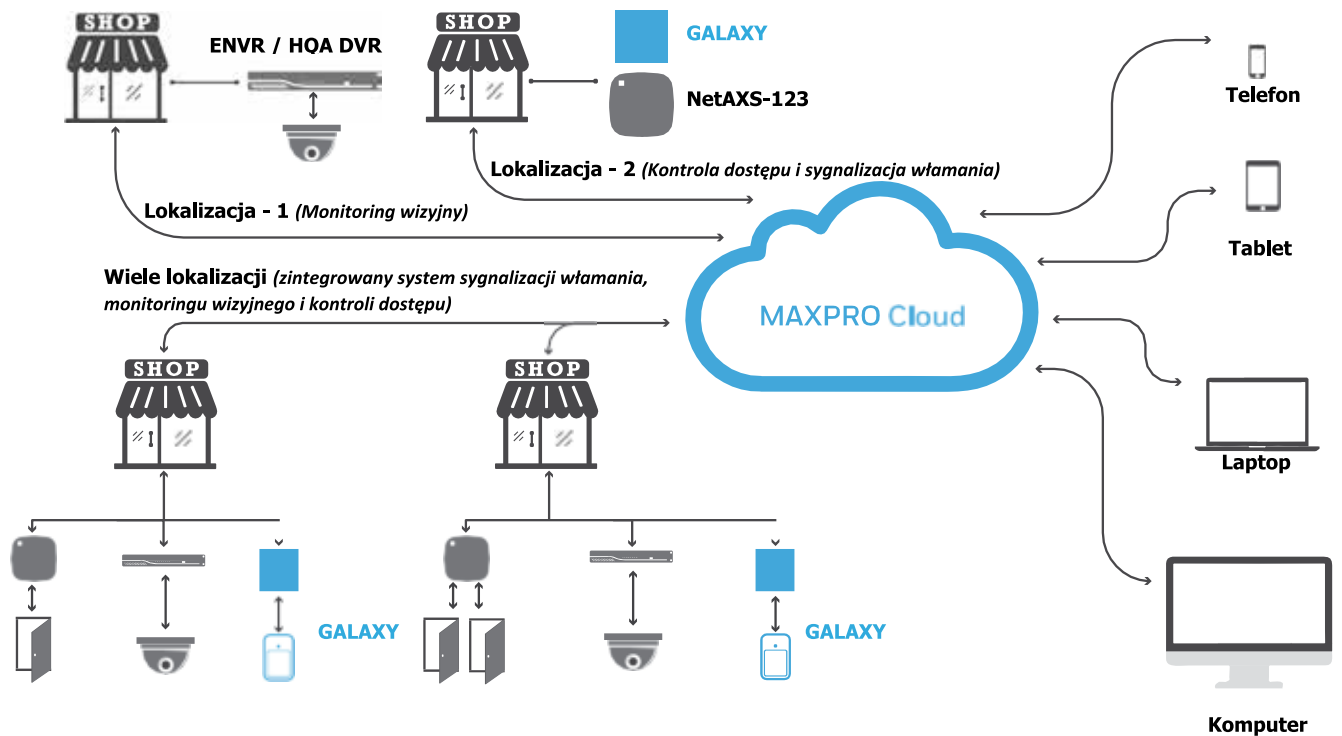
bezpieczeństwa, obniżenie kosztów instalacji oraz skrócenie czasu montażu.

Obsługa w chmurze zapewnia skalowalność, możliwość łatwej rozbudowy oraz wydajność – nie są wymagane serwery ani oprogramowanie, co znacznie redukuje koszty infrastruktury IT oraz zakupu oprogramowania.

Intuicyjny interfejs użytkownika składa się z dynamicznych pulpitów nawigacyjnych, nakładki Google Maps oraz dostosowywanych map obiektów. Posiada funkcję przeglądu zdarzeń alarmowych, kontroli dostępu, nagrań oraz monitorowania alarmów i zdarzeń w czasie rzeczywistym. Raporty mogą być generowane automatycznie lub na żądanie i wysyłane na adres e-mail.

Wydajna aplikacja mobilna zapewnia widok ogólny, widok kondycji, stanu i zdarzeń oraz zarządzanie systemami alarmowym, kontroli dostępu i monitoringu wizyjnego dla wielu obiektów (załą-





Zintegrowany system monitoringu wizyjnego, sygnalizacji włamania i kontroli dostępu obsługujący wiele obiektów

czenie i wyłączenie systemu, zarządzanie dostępem użytkownika, zdalne blokowanie i odblokowanie przejścia, odtwarzanie nagrań oraz wysyłanie powiadomień do użytkownika)

Korzyści dla instalatora

- Niższe koszty i krótszy czas instalacji dzięki strukturze typu „plug and play”
- Większa wydajność i niższe koszty eksploatacji dzięki możliwości zdalnej kontroli systemu i wykrywania ewentualnych awarii
- Konfiguracja kont, obiektów, harmonogramów i użytkowników – oszczędność czasu instalacji na obiekcie
- Aktualizacja oprogramowania sprzętowego z poziomu chmury, bez konieczności dojazdu na obiekt

Korzyści dla klienta

- Redukcja fałszywych alarmów dzięki weryfikacji zdarzeń
- Większa wydajność i niższe koszty eksploatacji dzięki możliwości przystosowania systemu do potrzeb firmy
- Dostęp z dowolnego miejsca, możliwość szybkiego podejmowania przemyślanych decyzji
- Zarządzanie wieloma lokalizacjami dzięki funkcji logowania się jednego użytkownika do wszystkich obiektów

- Zdarzenia alarmowe i dostępu z funkcją weryfikacji wideo

Ochrona danych

Honeywell wdrożył w MAXPRO Cloud zarówno techniczne, jak i organizacyjne środki bezpieczeństwa, aby pomóc użytkownikowi końcowemu w spełnieniu wymogów RODO.

Techniczne środki bezpieczeństwa obejmują bezpieczne logowanie HTTPS, szyfrowanie 256-bitowe oraz centra danych o wysokiej dostępności.

Zapora Honeywell wdrożona na platformie Microsoft Azure rozszerza zabezpieczenia infrastruktury chmury Azure i zapobiega atakom sieciowym oraz naruszeniom bezpieczeństwa danych, zapewniając jednocześnie bezpieczną łączność ze środowiskami chmury publicznej Azure.

Zawiera ona system zapobiegania włamaniom (IPS), zapewniający kompleksową ochronę sieci przed złośliwym i niechcianym ruchem sieciowym, w tym atakami złośliwego oprogramowania, atakami Dos i DDoS, podatnościami na aplikacje i serwery oraz zagrożeniami związanymi z wykorzystaniem informacji poufnych.

Urządzenia są dostarczane ze wstępnie skonfigurowanymi adresami URL, aby umożliwić łatwą instalację i nawiązać połączenie z chmurą. Oddzielne instancje chmurowe są skonfigurowane na rynki

europejskie w celu spełnienia wymagań prawnych i wymogów dotyczących prywatności danych.

Zaimplementowano globalne kierowanie ruchem, które może inteligentnie kierować ruchem z urządzeń na podstawie zainstalowanej lokalizacji do odpowiednich regionalnych instancji chmury.

Organizacyjne środki bezpieczeństwa obejmują zarządzanie rejestrami, kontami, procedury weryfikacji i zarządzanie dostępem.

Dzięki Honeywell MAXPRO Cloud klient może prowadzić rejestr przetwarzania danych i bezpiecznie przechowywać dane w bezpiecznym miejscu, aby zapobiec wyciekowi poufnych informacji. Dostęp do przechowywanych danych jest kontrolowany przez standardowe polityki bezpieczeństwa.

Rozwiązanie Honeywell MAXPRO Cloud pozwala użytkownikowi końcowemu na wybór czasu przechowywania nagrań wideo, poświadczeń, alarmów oraz zdarzeń kontroli dostępu. Proces ten jest kontrolowany i może być modyfikowany przez użytkownika, poprzez wybór odpowiednich pakietów licencyjnych i zdefiniowanie ich w profilach użytkowników. Efektem jest całkowite usunięcie danych z chmury po określonym czasie przechowywania. ■

Artykuł Firmowy
TAP Systemy Alarmowe

UMOWA O ZAKAZIE KONKURENCJI NA GRUNCIE PRAWA PRACY

Wstęp

W dobie społeczeństwa informacyjnego i szybkiego postępu technologicznego, dla przedsiębiorcy coraz większe znaczenie mają kwestie związane z posiadaniem przez firmę kapitałem ludzkim oraz know-how. Posiadanie przez przedsiębiorcę unikatowej technologii oraz pracowników zdolnych do jej wdrożenia i wykorzystywania często pozwala uzyskać znaczącą przewagę nad rynkowymi konkurentami. Niestety takie unikalne technologie oraz know-how w relatywnie łatwy sposób mogą znaleźć się w posiadaniu konkurencyjnych podmiotów, na przykład na skutek przejścia pracownika. Dlatego obecnie coraz istotniejszym jest aby przedsiębiorca odpowiednio zabezpieczył swój interes, w tym poprzez zawieranie umów o zakazie konkurencji ze swoimi kluczowymi pracownikami.

W tym kontekście warto mieć na uwadze, że kodeks pracy zawiera w tej materii pewne postanowienia, które ograniczają możliwość swobodnego kształtowania treści umów o zakazie konkurencji, a które trzeba uwzględnić, aby mieć pewność, iż wprowadzone do umowy postanowienia są ważne i w sposób rzeczywisty chronią interesy przedsiębiorcy. W niniejszej publikacji zostaną zaprezentowane w sposób skrótowy najważniejsze informacje dotyczące możliwości wprowadzenia zakazu konkurencji, zarówno w trakcie trwania stosunku pracy, jak i po jego zakończeniu.

Umowa o zakazie konkurencji w trakcie trwania stosunku pracy

Omawiając kwestię umowy o zakazie konkurencji w trakcie trwania stosunku pracy, należy nadmienić, że nawet jeśli pracodawca nie zawarł z pracownikiem stosownej umowy w tej materii, to i tak zgodnie z kodeksem pracy do obowiązków pracownika należy dbanie o dobro zakładu pracy, chronienie jego mienia oraz zachowywanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (art. 100 § 2 pkt 4 k.p.).

Część prawników i sądów stoi na stanowisku, że z samego obowiązku dbania o dobro zakładu pracy wynika konieczność powstrzymywania się przez pracownika od działalności konkurencyjnej, więc nawet jeśli nie została zawarta umowa o zakazie konkurencji w trakcie trwania stosunku pracy, to podjęcie takiej działalności przez pracownika uzasadnia wypowiedzenie umowy o pracę, a w pewnych szczególnych przypadkach nawet dyscyplinarne zwolnienie pracownika.

Należy mieć jednak na uwadze, że część prawników prezentuje pogląd odmienny nie widząc możliwości rozwiązania z pracownikiem umowy w związku z podjęciem przez niego działalności konkurencyjnej, jeśli nie została zawarta umowa o zakazie konkurencji, dlatego też z punktu widzenia przedsiębiorcy bezpieczniej jest, aby taka umowa została zawarta.

Mając powyższe na uwadze, przechodząc do umowy o zakazie konkurencji w trakcie trwania stosunku pracy należy wskazać, że tą kwestię normuje przede wszystkim art. 101¹ k.p. oraz następne, zgodnie z którymi pracodawca może zawrzeć z pracownikiem odrębną umowę w formie pisemnej zgodnie z którą pracownik nie może prowadzić działalności konkurencyjnej względem pracodawcy, ani też świadczyć pracy w ramach stosunku pracy lub na innej podstawie, na rzecz podmiotu prowadzącego działalność konkurencyjną. W przypadku naruszenia zakazu pracodawca może dochodzić od pracownika naprawienia szkody na zasadach określonych w kodeksie pracy.

Mając na uwadze treść przywołanych przepisów kodeksu pracy należy w pierwszej kolejności zwrócić uwagę, że umowa o zakazie konkurencji powinna zostać koniecznie zawarta w formie pisemnej pod rygorem nieważności, inaczej niż ma to miejsce w przypadku umowy o pracę, która może skutecznie zostać zawarta w formie dorozumianej, a jedynie powinna zostać potwierdzona w formie pisemnej.

Co istotne kodeks pracy wskazuje, że zakaz konkurencji powinien zostać zawar-

ty w odrębnej umowie, a więc najlepiej aby był to odrębny dokument. W prawie większość prawników i sądów stoi na stanowisku, że umowa o pracę oraz umowa o zakazie konkurencji mogą znajdować się w jednym dokumencie, ale ze względu na fakt, że część prawników prezentuje odmienny pogląd, bezpieczniej jest zawrzeć umowę o zakazie konkurencji w odrębnym dokumencie od umowy o pracę.

Umowa o zakazie konkurencji może zostać zawarta zarówno w momencie nawiązania stosunku pracy, jak i w jego trakcie. Oczywiście najlepszym rozwiązaniem jest aby umowa o zakazie konkurencji była podpisywana w momencie zawierania umowy o pracę, kiedy pracodawca ma największą możliwość skłonienia przyszłego pracownika do podpisania takiej umowy. Nie mniej jednak również w trakcie trwania stosunku pracy pracodawca ma argumenty, aby przekonać pracownika do podpisania takiej umowy, ponieważ zgodnie z poglądami części prawników i sądów odmowa podpisania umowy o zakazie konkurencji w trakcie trwania stosunku pracy może stanowić podstawę do wypowiedzenia umowy o pracę chyba, że treść proponowanej umowy jest niezgodna z przepisami prawa pracy.

Umowa o zakazie konkurencji nie musi być odpłatna, ale nic nie stoi na przeszkodzie aby strony wprowadziły dodatkowe wynagrodzenie z tego tytułu.

Istotnym elementem umowy o zakazie konkurencji jest precyzyjne określenie zakresu zakazu konkurencji. Im dokładniej zostaną sformułowane postanowienia umowne w tej materii, tym łatwiej strony będą w stanie uniknąć ewentualnych sporów sądowych na tym tle. Zakaz konkurencji może dotyczyć w szczególności ograniczeń w prowadzeniu działalności konkurencyjnej, uczestnictwa w organach podmiotów konkurencyjnych, uczestnictwa w tworzeniu przedsiębiorstw konkurencyjnych, posiadania udziałów konkurenta, czy też wchodzenia w stosunki prawne z klientami pracodawcy. Warto mieć na uwadze, że zupełny brak okre-

ślenia zakresu zakazu konkurencji może skutkować nieważnością umowy o zakazie konkurencji.

Z drugiej jednak strony zakres zakazu konkurencji, powinien pozostawać w związku z rzeczywiście prowadzoną przez pracodawcę działalnością. Jeżeli zakres zakazu konkurencji zostałby określony zbyt szeroko, to taka umowa może być częściowo lub całkowicie nieważna. Przykładem zbyt szerokiego zakazu konkurencji może być całkowity zakaz wykonywania jakiegokolwiek działalności gospodarczej przez szeregowego pracownika lub zakaz wykonywania takiego rodzaju działalności gospodarczej, którą pracodawca ma wprawdzie wpisana jako przedmiot działalności w Krajowym Rejestrze Sądowym, ale której faktycznie nie wykonuje.

W orzecznictwie wskazuje się, że zakaz konkurencji w przypadku osób wchodzących w skład organów spółki (pracodawcy), może zostać sformułowany szeroko i w sposób bardziej ogólny, ze względu na szeroki dostęp do informacji istotnych dla funkcjonowania spółki.

Przechodząc do kwestii skutków naruszenia przez pracownika umowy o zakazie konkurencji w trakcie trwania stosunku pracy, to po pierwsze takie naruszenie może stanowić podstawę wypowiedzenia umowy o pracę, a niekiedy zwolnienia dyscyplinarnego. Po drugie taki pracownik może ponosić odpowiedzialność majątkową na zasadach określonych w kodeksie pracy w art. 114 k.p. – art. 122 k.p.. Odpowiedzialność materialna pracownika jest więc częściowo ograniczona, ponieważ zgodnie z ww. przepisami, pracownik w przypadku nieumyślnego naruszenia zakazu konkurencji, ponosi odpowiedzialność w zakresie rzeczywistych strat poniesionych przez pracodawcę (bez tzw. „utraconych korzyści”), co więcej jedynie do wysokości trzykrotności miesięcznego wynagrodzenia, natomiast w przypadku, gdy szkoda zostanie wyrządzona umyślnie pracownik ponosi nieograniczoną odpowiedzialność za wyrządzoną szkodę.

Niestety zgodnie z orzecznictwem sądowym niedopuszczalne jest zastrzeżenie kary umownej na wypadek naruszenia przez pracownika zakazu konkurencji w trakcie trwania stosunku pracy, co znacznie ułatwiłoby ewentualne postępowania sądowe przeciwko nieuczciwym pracownikom, ponieważ zdejmowałoby z pracodawcy obowiązek wykazywania wielkości poniesionej szkody.

Umowa o zakazie konkurencji po ustaniu stosunku pracy

Kwestię umowy o zakazie konkurencji po zakończeniu stosunku pracy normuje przede wszystkim art. 101² k.p., który odsyła częściowo do unormowań dotyczących zakazu konkurencji w trakcie trwania stosunku pracy tj. art. 101¹ § 1 k.p., przez co niektóre elementy dla obu rodzajów umów są wspólne.

W obu przypadkach do zawarcia umowy wymagane jest zachowanie formy pisemnej pod rygorem nieważności, co więcej ze względu na treść przepisów bezpieczniej jest zawrzeć umowę w odrębnym dokumencie, a nie łącznie z umową o pracę, choć większość sądów dopuszcza aby zakaz konkurencji po ustaniu stosunku pracy znajdował się w tym samym dokumencie, co umowa o pracę.

Ponadto w przypadku obu rodzajów umowy wymagane jest wskazanie zakresu zakazu konkurencji, który powinien być w miarę możliwości konkretny w przypadku pracowników niższego szczebla, a może być bardziej ogólny (szeroki) w przypadku członków organów spółki (pracodawcy). Zakres zakazu konkurencji powinien być ograniczony do obszarów działalności pracodawcy, gdzie istnieje rzeczywiste ryzyko prowadzenia działalności konkurencyjnej, a więc w przypadku zbyt szerokiego określenia zakresu zakazu, pracodawca musi liczyć się z tym, że umowa będzie częściowo lub całkowicie nieważna.

Jeżeli chodzi o elementy odróżniające oba typy umów o zakazie konkurencji, to należy wskazać na takie okoliczności jak: czas obowiązywania, kwestia odpłatności, zakres podmiotowy, zakres odpowiedzialności pracownika za jej naruszenie.

Obojętnym elementem umowy o zakazie konkurencji po zakończeniu stosunku pracy niezbędnym dla jej ważności jest wskazanie przez jaki czas będzie ona obowiązywać. W praktyce takie umowy są zawierane na okres jednego roku, ale nic nie stoi na przeszkodzie, aby strony ustaliły dłuższy okres, w szczególności jeżeli taka potrzeba wynika ze specyfiki danej branży.

Należy zwrócić uwagę, że niezależnie od okresu obowiązywania zakazu wskazanego w umowie, to zgodnie z art. 101² § 2 k.p. zakaz konkurencji przestaje obowiązywać przed upływem terminu, na jaki została zawarta umowa, w razie ustania przyczyn uzasadniających taki zakaz lub niewywiązywania się pracodawcy z obowiązku wypłaty odszkodowania.

Umowa może również ulec wcześniej- szemu zakończeniu na skutek pisemnego porozumienia stron, a także jednostronnego jej wypowiedzenia lub odstąpienia, pod warunkiem, że takie sposoby rozwiązania umowy zostały przewidziane w samej umowie. Wśród prawników dominuje pogląd, że do skutecznego zastrzeżenia możliwości odstąpienia (wypowiedzenia) umowy o zakazie konkurencji przez pracodawcę, nie jest niezbędne wskazywanie konkretnych okoliczności, w których takie odstąpienie (wypowiedzenie) może nastąpić.

Kolejnym elementem odróżniającym oba rodzaje umowy, jest kwestia obojętnego odszkodowania (wynagrodzenia), w przypadku zakazu konkurencji po zakończeniu stosunku pracy, które zgodnie z kodeksem pracy musi wynosić co najmniej 25% wynagrodzenia otrzymanego przez pracownika przed ustaniem stosunku pracy przez okres odpowiadający okresowi obowiązywania zakazu konkurencji, wypłacanego w ratach miesięcznych lub jednorazowo.

Należy zauważyć, że brak wskazania takiego wynagrodzenia w umowie nie skutkuje nieważnością umowy o zakazie konkurencji po zakończeniu stosunku pracy, a jedynie w miejsce nieważnego postanowienia wchodzi ww. postanowienie ustawowe o odszkodowaniu. Oczywiście odszkodowanie może zostać ustalone w wyższej kwocie, niż przewidziano w kodeksie pracy.

Umowa o zakazie konkurencji po zakończeniu stosunku pracy, co do zasady może zostać zawarta z pracownikiem, który miał lub mógł mieć dostęp do szczególnie ważnych informacji dla pracodawcy. Nie oznacza to jednak, że pracownik po jej zawarciu może kwestionować ważność takiej umowy twierdząc, że nie miał dostępu do takich informacji.

Przechodząc do kwestii naruszenia przez pracownika zakazu konkurencji po ustaniu stosunku pracy, po pierwsze należy wskazać, że zgodnie z orzecznictwem takie naruszenie uprawnia byłego pracodawcę do wstrzymania wypłat dalszych rat odszkodowania. Ponadto, jeśli na skutek zakazu konkurencji pracodawca odniósł szkodę, to może on dochodzić od pracownika odszkodowania w pełnej wysokości na zasadach wynikających z kodeksu cywilnego tj. z tytułu niewykonania lub nienależytego wykonania zobowiązania (art. 471 k.c. i następane).

Co istotne z punktu widzenia interesów pracodawcy, w tym rodzaju umowy

o zakazie konkurencji, dopuszczalne jest zastrzeżenie kary umownej, co znacząco ułatwia ewentualne postępowanie sądowe, gdyż pracodawca nie jest w takiej sytuacji zmuszony wykazywać istnienia i wielkości poniesionej szkody na skutek naruszenia umowy o zakazie konkurencji.

Zakończenie

Na zakończenie należy wskazać, że niniejszy artykuł ze względu na swoją objętość stanowi jedynie ogólne omówienie kwestii związanych z zakazem konkurencji. Niezależnie od przywołanych przepisów

pomocna w ochronie interesów pracodawcy względem nieuczciwego pracownika może być również ustawa o zwalczaniu czynów nieuczciwej konkurencji, która normuje kwestie związane z zachowaniem przez pracownika tajemnicy przedsiębiorstwa, zarówno w trakcie trwania stosunku pracy, jak i po jego zakończeniu.

Ponadto należy zwrócić uwagę, że w przypadku współpracy z osobami fizycznymi na podstawie innych umów niż umowa o pracę, np. umowy zlecenia, strony mają nieco większą swobodę w zakresie normowania kwestii związanych z zakazem konkurencji.

Radostaw Monia

Absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego oraz kierunku Międzynarodowe Stosunki Gospodarcze w Szkole Głównej Handlowej w Warszawie. Ukończył aplikację radcowską w Okręgowej Izbie Radców Prawnych w Warszawie. Obecnie współpracuje z Kancelarią LTA Doradztwo Prawne Dopierata i Wspólnicy sp. komandytowa oraz prowadzi własną kancelarię prawną. Specjalizuje się w prawie cywilnym oraz gospodarczym.

ZARZĄDZANIE | OCHRONA TAJEMNIC FIRMY PRZED WEWNĘTRZNYM WROGIEM

TWÓJ WSPÓŁPRACOWNIK – TWÓJ WRÓG

Jakiś czas temu w prasie można było przeczytać, jak pewna firma spedycyjna, działająca w Trójmieście, nie musiała się domyślać, gdyż utratę pierwszych sześciu najważniejszych klientów i pół miliona złotych szybko skojarzyła z odejściem czterech pracowników, którzy zatrudnili się w przedstawicielstwie szwedzkiej konkurencji. Posługiwali się oni szczegółami dotyczącymi kontraktów, jakie ich były pracodawca zawarł z kontrahentami, tras przejazdów itd., mimo że podpisali wcześniej umowy o zakazie konkurencji i zachowaniu poufności informacji przez trzy lata od ustania stosunku pracy. Niestety, prokuratura odmówiła wszczęcia dochodzenia, gdyż firma nie mogła przedstawić „twardych dowodów”. Jej pliki, znalezione przez policję w komputerach konkurencji, nie miały znaczenia, bo podejrzani po prostu zaprzeczyli, że je wykradli. W Szwecji samo posługiwanie się takimi plikami wystarczyłoby, aby zamknąć nieuczciwe przedsiębiorstwo, ale u nas prawo o konkurencji jest tak skonstruowane, że bardzo trudno pociągnąć kogoś do odpowiedzialności karnej (prokuratura wszczyła dochodzenie tylko w kilku procentach zgłoszonych przypadków). Pozostaje droga cywilna, której firmy zazwyczaj unikają,

gdyż jest długa i kosztowna. Poza tym informacja o tym, że firma dała się oszukać, co może wypłynąć do opinii publicznej, może zachęcić innych. Albo wygenerować kolejne straty, tym razem wizerunkowe. Przez to właśnie kradzież poufnych danych jest w Polsce tak nagminna – złodzieje często czują się bezkarni.

Kiedyś trafił do mnie do analizy wniosek pewnej nowej firmy, która zaczynała od przysłowiowego „zera”. Szukali oni finansowania i trafili do mnie abym pomógł im te pieniądze znaleźć. Gdy rozmawialiśmy, klienci od razu uprzedzili, że są byłymi pracownikami jednej z polskich firm, odpowiedzialnych za serwisy pewnych skomplikowanych urządzeń. Postanowili odejść z firmy, gdyż poczuli się w niej okradani i wykorzystywani. Ale nie odeszli z pustymi rękami – tworząc nową firmę – nastavili się na kontynuowanie tego samego co robili na etacie w poprzednim miejscu zatrudnienia. Ba! Nawet skierowali swoją ofertę do klientów swojej byłej firmy, oferując swoje usługi za zdecydowanie mniejsze pieniądze. Naprawdę nie trzeba być przenikliwym analitykiem, by przewidzieć, jak bolesne dla byłego pracodawcy było odejście ich komórki serwisowej.

Niestety bardzo trudne jest zabezpieczenie się przed kradzieżą tajemnic firmy przez pracowników. Tak naprawdę każde przedsiębiorstwo, które ceni sobie własne osiągnięcia, tajemnice firmy, bazę swoich klientów z chwilą zatrudnienia pracownika powinna się już zabezpieczyć przed sytuacją, kiedy zatrudniony może chcieć działać na niekorzyść firmy a co gorsza, skuszony ofertami konkurencji pomyśli, by działać na jej rzecz albo celowo sabotować działania firmy, która go zatrudnia. Dlatego przy zdecydowaniu o zwiększonej fluktuacji zatrudnienia, wiele firm decyduje się przy podpisywaniu umowy o pracę, równocześnie zawrzeć w umowie zapisy chroniące firmę przed tego typu działaniami. Umowa o unikaniu działań na szkodę przedsiębiorstwa oraz na rzecz konkurencji od razu wprowadza pracownika w brutalną rzeczywistość biznesową: zatrudniający zabezpiecza swoje tajemnice i dobro firmy zaś kandydat do pracy wie, że firma będzie podejmować wszelkie działania, by chronić to co jest jej najcenniejszym dobrem i jeśli pracownik złamie stosowne zabezpieczenia i zacznie działać na szkodę firmy, będzie wiedział, jakie go będą czekać tego konsekwencje. Jasny



układ – ja, jako właściciel firmy szkole Cię, inwestuję w Ciebie, daję Ci pieniądze, chronię Ciebie, byś dla mnie uczciwie pracował – ale jeśli zaczniesz mi szkodzić, odzyskam wszystko i doprowadzę Cię do poniesienia konsekwencji tego, iż zdradziłeś naszą firmę, swoich współpracowników i zawiodłeś nasze nadzieje – tak mniej więcej powinna wyglądać szczerza rozmowa z wprowadzanym do firmy nowym pracownikiem. Ja szkoląc firmy z radzenia sobie z problemem oszustw wewnętrznych oraz nielojalności pracowników zawsze zachęcałem do jasnych zasad i przedstawiania w sposób otwarty reguł chroniących przedsiębiorstwo. Skutkowało to tym, że gdy sprawa nielojalnego pracownika trafiała do sądu, były menadżer czy pracownik nie mógł zaprzeczać, że o niczym nie wiedział działając na szkodę firmy. Prawnik okradzonego przedsiębiorstwa wyciągał zawsze tzw. „cyrograf” – umowę o unikaniu działania na rzecz konkurencji i przedsiębiorstwa, gdzie przy przyjęciu do firmy własnym podpisem każdy kandydat do pracy potwierdzał, że zapoznał się z zasadami ochrony informacji, że wie jakie są zastosowane rozwiązania monitorujące jego pracę, oraz jakimi procedurami ma się kierować, by nie dopuścić do

działań szkodliwych dla firmy. Dlatego firmy stosujące to rozwiązanie miały zdecydowanie mniej problemów z nierzetelnymi pracownikami czy menadżerami. To jednak nie wystarcza.

Zadziwiające jest, jak w wiele firm działa bez świadomości, że każdy zatrudniony w firmie – od członków zarządu po sprzątaczkę, może w każdej chwili z kogoś komu się ufa przejść do pozycji największego zagrożenia dla firmy.

Zajmując się od lat 90-tych dbaniem o bezpieczeństwo firm wiedziałem, że wbrew pozorom największe zagrożenie dla przedsiębiorstw tkwi w ich organizacji.

Truizmem już jest twierdzenie, że „najsłabszym ogniwem w każdym systemie i organizacji jest człowiek”. Dzisiaj wszystkie straty jakie ponoszą firmy, można sprowadzić do pojęcia nadużycia pracowniczego – czy narażającym na straty jest ktoś z zewnątrz, czy jest to kontrahent, współnik, dostawca, klient – zawsze w tym działaniu szkodzącym firmie uczestniczy ktoś z naszej firmy. Czy jest to działanie dobrowolne czy czysta głupota, czy jest to współudział czy działanie sprawcze, do którego zaangażowano kogoś z zewnątrz, rzadko zdarza się, by w danym nadużyciu wobec firmy nie uczestniczył ktoś z samej

firmy. Cokolwiek złego się zdarzy – gdzieś zawsze zaangażowany jest w to pracownik – obecny lub były.

Jak więc sobie z tym problemem radzić?

Już świadomość tego, iż Wasza firma może być narażona na straty z powodu działań nieuczciwych pracowników, jest dobrym sygnałem. Niestety tylko około 80% firm ma świadomość zagrożeń ze strony pracowników. Tworzymy firmę, pracownicy się zżywają, firmy bardzo dużo inwestują w to, by wszyscy w firmie czuli się jak w rodzinie. Ale zapomina się przy tym, że nawet w najlepszych rodzinach zdarzają się zdrady i kłótnie, które powodują, że ktoś kto do tej pory był nam najbliższy, nagle staje się naszym zajądłym wrogiem.

Symptomy kryzysu

Gdy nagle dostrzegamy brak chęci do pracy, gdy zaczynamy odnotowywać spadek wydajności po stronie zatrudnionych, dostrzegalna jest zwiększająca się absencja, częste branie „wolnych dni”, odnotowuje się spóźnienia i tzw. urywanie się z pracy, a zmorą stają się częste prywatne telefony powodujące to, że pracownik znika z telefonem, wyłącza się z pracy w zespole a swoje obowiązki zaczyna spychać na innych; kiedy widzimy, że milknie, chowa się za plecami innych, obojętnieje a na samym końcu zaczyna się pojawiać w pracy nagle bez powodu bardziej elegancko ubrany – wtedy z wielkim prawdopodobieństwem możesz być pewny, że Twój pracownik właśnie szykuje się do odejścia. Sporo osób bagatelizuje ten moment. Ale jeśli nie wiesz czemu odchodzi z firmy, co go do tego pchnęło narażasz się na kłopoty. Bo jeśli pracownik czuje się mobbowany, skrzywdzony, oszukany, „okradziony przez firmę”, to pojawia się dla niego motyw, który może go skłonić do działania na szkodę firmy. W tym czasie kopiować może twoje dane, przekazywać istotne informacje konkurencji, może kopiować bazy twoich klientów – ba! Może się z nimi spotykać, na Twój koszt, mówić im rzeczy, które twoją firmę stawiają w fałszywym i niekorzystnym świetle i pozwoli przejmować ich na rzecz nowego już pracodawcy. Takie działania będzie sobie uzasadniał i racjonalizował poczuciem krzywdy, jaką może odczuwać. Gdy jeszcze ma okazję do działania, które przynosi mu korzyści, spełnia jego chęć zemsty,

daje mu satysfakcję, bo „dokopuje tym, którzy go nie doceniali, nie wspierali albo krzywdzili” – firma jest już w sporych kłopotach. Gdy trafiały do mnie informacje o mobbingu wiedziałem, że tam, gdzie sugerowano działanie mobbera, prawdopodobieństwo nadużyć i działań na szkodę firmy wzrastało niewspółmiernie wysoko. Dlatego jeśli otrzymujesz anonimowy o mobbingu, nie bagatelizuj takich sygnałów. Od razu badaj, co się dzieje, bo prawdopodobnie jest chociaż jedna osoba skrzywdzona, która w poczuciu krzywdy, może skorzystać z okazji by „zemścić” się w sposób, który może być dla firmy bardzo bolesny.

Symptomów wskazujących, że masz problemy z nieuczciwością pracowniczą jest cała lista: spadek sprzedaży oraz rosnące koszty działania firmy, szczególnie te związane z pracownikami i kosztami ich podróży służbowych, dojazdów, kosztów paliwa w ich samochodach służbowych czy kosztów związanych z bieżącą działalnością. Poza absencją i spadkiem efektywności, pojawiają się też inne – jak tworzenie nieformalnych układów w firmie, szczególnych i niedopuszczających nikogo postronnego. Ten wzrost kosztów jeśli nie jest badany powoduje, że zaczynają one rosnąć a w długim przedziale czasu sprzyjają poczuciu bezkarności pracownika. To takich ludzi motywuje do podejmowania kolejnych działań, dających im korzyść a generujących kolejne straty. Wzrost majątności pracownika, nieadekwatny do jego zarobków, częste wyjazdy zagraniczne, zmiana samochodu na lepszy, wyższy standard życia – to są sygnały, które warto sprawdzić. Często intuicja, te słynne „palące się czerwone lampki” w głowach przełożonych, powinny być powodem do przyjrzenia się pracownikom i ich działaniom pod kątem generowanych dla firmy ryzyk.

Ufaj, ale kontroluj

Dzisiaj standardem w niektórych sektorach gospodarki jest stały monitoring działań pracowników i menadżerów. Monitorowanie służbowych komórek, poczty korporacyjnej, działań w internecie prowadzonych w godzinach pracy, a nawet monitorowanie przemieszczania się pracowników w miejscu i otoczeniu pracy, to wszystko służy ochronie firmy przed działaniami na niekorzyść przedsiębiorstwa. Nowe wymogi RODO nakładają obowiązki zabezpieczania i dbania o dane osobowe, w tym dane klientów i samych

pracowników. By je chronić, trzeba monitorować także działania pracowników.

Firmy chcąc dbać o dobro klientów i pracowników, monitorują działania pracowników, by optymalizować koszty prowadzonej działalności. Chcąc wygrać z konkurencją, muszą chronić swoje dane, dane klientów, planowane działania i strategie biznesowe a także oszczędzać.

Jeśli pozwalasz na wszystko, wszystko możesz stracić

Wielu właścicieli firm obawia się zaostrezenia kursu i sięgania po rozwiązania utrudniające nieuczciwe działania pracowników. Jeden z prezesów powiedział mi wprost: „Wiesz, ja wiem, że moi pracownicy podkradają mnie. Ale ja to traktuję jako pewien bonus, bo chociaż tracę na tym co mi zabierają, to jestem zadowolony z tego, że zarabiają dla mnie niezłe pieniądze. Ja sobie straty wpisuję w koszty, ale dzięki temu moja firma przynosi nienajgorszy dochód”. Kiedy mi to powiedział spojrzałem na niego i zwróciłem uwagę na kilka faktów. Tolerując nieuczciwość pracowników, wzrastają mu koszty działalności a przez to, staje się mniej konkurencyjny. Za jakiś czas, taka polityka spowoduje zwiększenie strat i zmniejszenie zysków. Na samym końcu zwykle dochodzi do dużej straty i utracenia przewagi konkurencyjnej. Bo jeśli ktoś nic nie robi, albo nie robi wiele, by ograniczać kradzieże, wypływ danych do konkurencji, wyłudzenia i oszustwa po stronie pracowników, rozzuchwala w ten sposób i demoralizuje pracowników oraz kadrę menadżerską do tego stopnia, że w dłuższym przedziale czasu straty z tytułu nieuczciwości pracowniczej zabierają nawet wieloletnie zyski. Są firmy, które z tego powodu znikły już z rynku, straciły reputację a wielu ich właścicieli musiało swoje nawet latami budowane firmy sprzedać konkurentom. Nieuczciwość po stronie zatrudnianych to ryzyko, które potrafi doprowadzić do poważnych kryzysów. Nie chcę tu wskazywać

palcem firm, które dzisiaj niewiele znaczą na rynku, a kiedyś były podmiotami „rządzącymi” na rynku. Do „zmiany liderów” doprowadzili ci, którzy przeoczyli ten moment, w którym nieuczciwy menadżer lub pracownik stworzył zagrożenie dla firmy zagrożenie.

Już dzisiaj istnieją odpowiednie rozwiązania, które minimalizują ryzyko, o którym wyżej napisałem. Stworzyłem wiele komórek antyfraudowych, które zajmowały się inwestygowaniem stwierdzonych zagrożeń dla funkcjonowania przedsiębiorstwa. Dobierałem moim klientom rozwiązania, pozwalające na rozpoznanie nie tylko nieuczciwych pracowników, generujących zagrożenia i straty dla firm, ale również działających celowo, by przedsiębiorstwa osłabić albo pomóc w ich oszukaniu. Dzisiaj tylko od woli zarządzających firmą zależy, czy chcą oni się bronić przed nieuczciwością pracowników i ich działaniem czy sobie to odpuszczają. Oszczędzanie w tej materii jest działaniem na szkodę firmy. Inwestowanie w przeciwdziałanie wewnętrznym oszustom, szybko się zwraca: eliminuje się szkodliwe osoby, obniża się koszty poprzez ukrócenie nadużyć i okradania firm przez nietrzetelnych pracowników. Bardzo często dobrze dobrane narzędzia optymalizują działanie firm, urealniają sprzedaż, ograniczają straty i w ten sposób czynią firmy konkurencyjnymi. Dzisiaj, ktoś kto chce ścigać się z konkurencją, musi walczyć z wewnętrznymi „wrogami”. Bez tego naraża się tylko na straty a problemy co najwyżej przesuwają w czasie.

Jeśli Czytelniku doczytałeś do tego miejsca wiedz, że na każdą ww. sytuację możesz się przygotować. Bo dzisiaj wygrywają Ci, co przeciwdziałają nieuczciwości pracowniczej a nie czekają, aż ona się pojawi. Ale to, czy wygrasz z nieuczciwością zależy wyłącznie od Ciebie i tego kiedy podejmiesz decyzję, że nie dasz się oszukiwać. ■

Michał Czuma

Niezależny ekspert prowadzący własną firmę doradczą MC Consulting zajmującą się wspieraniem firm w sytuacjach kryzysowych. Od przeszło 20 lat zajmuje się tematyką oszustw oraz bezpieczeństwa inwestycji. Wcześniej przez 3 lata doradca zarządu, organizator i dyrektor Biura Przeciwdziałania Wyłudzeniom w PKO Leasing SA. W latach 2009–2014 pracował jako I zastępca dyrektora Departamentu Bezpieczeństwa PKO Banku Polskiego. W 2012 stworzył od podstaw Biuro Antyfraudowe PKO BP, którym później kierował przez 3 lata. Pracował jako ekspert odpowiedzialny za bezpieczeństwo inwestycji i doradca zarządu. Większość swojej drogi zawodowej poświęcił zagadnieniom bezpieczeństwa na styku z biznesem. Był managerem i doradcą w wielu firmach prywatnych i państwowych takich jak Poczta Polska, Bank Pocztowy, Bank Handlowy, PZU, RUCH S.A czy Emax S.A. Jako pełnomocnik Zarządu Hortex S.A odpowiadał za inwestycje na rynkach wschodnich i nadzorował m.in. bezpieczeństwo inwestycji na tamtym terenie w czasie najbardziej gorących wydarzeń politycznych, zachodzących w krajach byłego ZSRR. Absolwent Uniwersytetu Warszawskiego i ceniony od wielu lat ekspert ds. fraudów i bezpieczeństwa.

AUDYT BEZPIECZEŃSTWA OBIEKTU – TAJNA BROŃ ANALITYKA: METODYKA

Wybaczcie ale to, co stanowi wartość tej części serii artykułów o audycie bezpieczeństwa jest efektem nauki i pracy autora, w które włożył dobre 20 lat swojego życia. Autor nie bardzo zatem chce zdradzać wszystkie tajniki swojego warsztatu.

„Co zrobić, żeby zrobić”, czyli metodyka audytu bezpieczeństwa dla zaawansowanych

Ze względu na specyfikę obiektu (a przypomina się, że omawiamy audyt obiektu o znacznej komplikacji strukturalnej lub organizacyjnej), jego cyklu życia i istniejących systemów bezpieczeństwa, podczas realizacji audytu należy położyć bardzo mocny nacisk na precyzyjne formułowanie kolejnych kroków wykonawczych. One to są, a przynajmniej powinny być, podstawą do weryfikacji procesów, zasad, parametrów i stanu bezpieczeństwa. Uniwersalność takiej metodyki wymaga, by wykonawca (ale i odbiorca) w pełni rozumiał cel, w jakim wykonywane są kolejne czynności.

W związku z powyższym, omawiając tematykę przeprowadzania audytów, proponuje się omówienie następującej, autorskiej metodyki audytu.

Wstępna część opracowania

Podstawa opracowania

Ta część musi jasno definiować podstawę opracowania, tj.: rodzaj zawartej umowy i jej dane, jak też podstawy merytoryczne opracowania: wykonane wizje lokalne, wywiady, konsultacje, analizy oraz sprawdzenia. Konieczne jest również wyszczególnienie udostępnionych przez Zleceniodawcę materiałów, środków i sił niezbędnych oraz przypuszczalnych terminów wykonania prac.

Cel opracowania

Zdefiniowanie celu ogólnego, jaki został postawiony przed audytem obiektu, wynika z zamówienia Zleceniodawcy mającego najczęściej źródło w polityce bezpieczeństwa przedsiębiorstwa i pozwala na sprecyzowanie celów szczegółowych,

które przekładają się praktycznie jeden do jednego na zakres opracowania i konieczne są do zrealizowania każdego wymaganego obszaru audytu.

Uwagi i ograniczenia dotyczące opracowania

Jakość opracowania finalnego oraz jego wiarygodność wymaga wyznaczenia granic zawartych w nim badań, wywiadów, analiz i wniosków. W tym miejscu należy zawrzeć wszelkie ograniczenia wynikające z przyczyn formalnych, merytorycznych, metodologicznych, znanych w momencie przystępowania do wykonania opracowania. Również tych, które wyszły na jaw w trakcie pracy, a które będą miały bezpośredni i pośredni wpływ na ostateczny kształt i wnioski audytu.

To część, w której należy podać ograniczenia wynikające z jakości, formy i udostępnionego zasobu dokumentacji i informacji, czasu i sposobu ich pozyskania, ich dostępności, etc. Paradoks polega na tym, że najczęściej nie rozlicza się audytora z tego co zrobił, tylko z tego, czego NIE zrobił.

Tutaj też zamieszcza się używane skróty, które dla wygody i uproszczenia stosowane są w całym opracowaniu. Przyznacie, że łatwiej jest użyć terminu „NERO”, niż pełna nazwa Przedsiębiorstwa o dwujęzycznej nazwie „Zielona Kaskada. „Nero – Development” Spółka z ograniczoną odpowiedzialnością. Romanowski, Kiljańczyk i Partnerzy Spółka z ograniczoną odpowiedzialnością. Spółka komandytowa”¹.

Opis obiektu oraz jego najbliższego otoczenia

Charakterystyka funkcjonalna obiektu

Obligatoryjnie należy poświęcić dużą część pracy na zbudowanie platformy wiedzy i rozbudowanego kontekstu opracowania, którym będą dokładne opisy charakterystyki obiektu, podanie jego profilu funkcjonalnego oraz specyfiki działalności w nim prowadzonej, z podaniem wszystkich mieszczących się w nim podmiotów.

Opis i krótka charakterystyka każdego z obcych podmiotów mieszczących się na terenie naszego Klienta, jest rzeczą nader przydatną (dla autora tego tekstu – wręcz niezbędną), gdyż daje obraz komplikacji, zależności, specyfiki oraz naświetla utrudnienia mające bezpośredni wpływ na praktycznie wszystkie procesy ochronne audytowanego Przedsiębiorstwa.

Lecz przede wszystkim, w sposób maksymalnie precyzyjny należy tu zmieścić opis Obiektu. Bardzo dokładnie opisane (i zlokalizowane) miejsca, pomieszczenia, punkty, urządzenia i instalacje niewąlgiczne dla funkcjonowania i bezpieczeństwa obiektu, takie jak między innymi: ... (oj, to za dużo pisanie, a to przecież część dla zaawansowanych). Nie od rzeczy jest zasiegnięcie trochę wiedzy z BCP i BCM, gdyż informacje zawarte w tym podrozdziale, są jedną z najważniejszych podstaw do wyśnuwania wniosków pokontrolnych, a co najważniejsze – do ich uzasadnienia.

Wtręt niemerytoryczny nr 1

Od tego miejsca autor – z powodu chęci i konieczności zachowania tajemnicy zawodowej – będzie zawężał ilość ujawnianych tajników metodyki – oczywiście będzie pisał CO się powinno znaleźć w audycie (choć już nie tak obszernie), ale bez wyjaśniania JAK i uzasadnienia DLACZEGO.

Częściowy opis struktur pracowniczych oraz szczebli zarządczych obiektu

Opis obiektu, bez dokładnego opisu charakterystyki zatrudnienia podmiotu zarządzającego Obiektem, całkowicie mija się z celem – pozbawia obiekt i przedsiębiorstwa „życia”, które nadaje unikalny charakter dwóm, z pozoru takim samym organizacjom. A diabeł przecież, tkwi w szczegółach...

Należy tu uwzględnić wszelkie dane dotyczące ludzkiego aspektu, który może mieć Waszym zdaniem wpływ na szeroko rozumiane bezpieczeństwo obiektu, organizacji, przedsiębiorstwa. Bez tego audyt będzie pozbawiony tak samo wiarygodności, jak życia.

¹ Nazwa przedsiębiorstwa użyta przypadkowo, zaczerpnięta ze strony <https://www.komandytowa.pl/>.

Warto tu opisać wszelkie nieprawidłowości formalne, interpersonalne oraz pracownicze, o których audytor posiadał wiedzę z dostępnych mu źródeł oraz wskazać, jakie skutki mogą one ze sobą nieść.

Wtręt niemerytoryczny nr 2

Następujący po tej wstawce podrozdział, to kolejna najważniejsza część raportu... a jak dobrze się przyjrzeć, to im szerszy zakres audytu, tym więcej tych „najważniejszych” części, ale to tak trochę jak z klasówką z matematyki w podstawówce. Jeżeli nie napiszemy działań pośrednich pomiędzy zadaniem a wynikiem, to nauczyciel nam postawi pałę, niezależnie od trafienia (lub nie) w wynik końcowy. Tak też jest z Klientem – odbiorcą raportu poaudytowego. On nie ma obowiązku znać naszej branży, ale skoro ma podejmować decyzje niosące za sobą skutki organizacyjne i finansowe, to chce wiedzieć, z czego nasze zalecenia wynikają. I nie ma co się dziwić...

Infrastruktura obiektu

Ten fragment opracowania ma pokazać złożoność infrastrukturalną obiektu i występujące pomiędzy jej elementami różne współzależności. Jeżeli chcemy wzbogacić nasz raport o elementy graficzne (szkice, wykresy, plany, schematy i rzuty), to jest to odpowiednie miejsce.

To pierwsza z graficznych części opracowania – o ile zakres audytu wymaga takich części.

Otoczenie obiektu

Uzupełnieniem szczegółowego opisu funkcjonalnego obiektu oraz jego złożoności, jest niewątpliwie relacja z rozpoznania bliskiego – lecz proponujemy się nie ograniczać geograficznie – otoczenia tego obiektu. Każda informacja jest tu istotna, a każdy brak może okazać się brzemienisty w skutki i rzutujący zarówno na jakość finalnego opracowania jak i na wiarygodność audytora.

Przykład:

Przy analizie bezpieczeństwa lokalizacji dużej Organizacji, nie sprawdzono dokładnie otoczenia. Podjęto decyzję o rozbudowie oddziału i zainwestowaniu znacznych kwot. Po dłuższym czasie, podczas audytu BCM okazało się, że docieklawy (uparty i wścibski

– tak należałoby go nazwać) audytor zadał sobie trud i dotarł do sąsiadujących firm. Okazało się, że w jednej z nich jest przechowywana ponad tona amoniaku, co radykalnie zmieniło większość ocen zawartych w audycie. I spojrzenie managementu. I ocenę audytora dokonującego wstępnego audytu bezpieczeństwa lokalizacji.

Warto opisać wszystkie obiekty, procesy, urządzenia i specyficzne uwarunkowania (również społeczne), których istnienie i/lub funkcjonowanie może mieć wpływ na bezpieczeństwo analizowanego obiektu.

Opis zdiagnozowanych zagrożeń i ich analiza oraz ocena ryzyka

To jest rozdział opracowania, który nadaje sens i determinuje całą pozostałą zawartość raportu poaudytowego (znowu najważniejsza część...). Na podstawie zdiagnozowanych ryzyk, ocenionych zagrożeń oraz wypełnionej listy kontrolnej, którą dalej nazywam „Tabelą audytu bezpieczeństwa”, tworzy się część opisową, uzasadniającą oceny poszczególnych, audytowanych obszarów funkcjonowania Przedsiębiorstwa/Obiektu. Zawartość tej części przedstawiam poniżej w formie punktowej – każdy z tych punktów powinien zawierać szereg podpunktów, uszczegóławiających poszczególne grupy zagrożeń.

Wyszczególnienie i opis zagrożeń

- Naturalne (obiektywne)
- Wywołane przez człowieka (celowe)
- Wywołane przez człowieka (przypadkowe)

Zestawienie zagrożeń ocenionych

na wyższe niż akceptowalne²

Analiza w/w zagrożeń

Na przykładzie audytu obiektu produkcyjnego, autor wyszczególnia analizowane obszary. Każdy z nich można i powinno się rozwinąć, w celu transparentności opracowania. Są to:

- Cykl życia organizacji, zasoby ludzkie i ich organizacja
- Produkcja i jej podatności
- Produkt gotowy – cykl magazynowo logistyczny
- Komponenty, surowce i park narzędziowo-maszynowy
- Biura i działy wsparcia produkcji

² To zawsze jest – i powinien być – wybór audytora. Subiektywne spojrzenie stanowi w przypadku rzetelnego wykonawcy, wartość dodaną do opracowania.

- Bezpieczeństwo lokalizacji i infrastruktury (losowe i celowe), w tym katastrofy techniczne
- Zachowania społeczne
- Bezpieczeństwo fizyczne

Tabela oceny zagrożeń

Tabelę wykonujemy na matrycy oceny ryzyka, korzystając z oceny możliwości wystąpienia ryzyka i oszacowaniem potencjalnych skutków jego wystąpienia.

W efekcie dostajemy listę zagrożeń, z przypisaniem im czterostopniowej wartości:

Miara – liczona jako iloraz możliwości wystąpienia oraz potencjalnego skutku, wyskalowana jak poniżej:

E	Skrajne zagrożenie – zalecane wdrożenie programu zapobiegawczego PRZED incydem.
H	Wysokie zagrożenie – wymaga uwagi Kierownictwa. Zaleca się zmiany w procesach i procedurach.
M	Średnie zagrożenie – wymaga określenia odpowiedzialności za incydent i doraźnych decyzji.
L	Niskie zagrożenie – sytuacja zarządzana procedurami standardowymi.

Tabela audytu bezpieczeństwa Obiektu

Wszystkie opisane w „Tabeli oceny ryzyka” i zweryfikowane w „Tabeli audytu bezpieczeństwa” zakresy, powinny być w następnych częściach szczegółowo opisane. Stanowią podstawę do formułowania wniosków pokontrolnych i budowania zaleceń (proponycji naprawy stanu zastanego).

Część opisowa opracowania

Teraz następuje żmudne, lecz niezbędne opisywanie każdego z wyszczególnionych w Tabeli oceny ryzyka obszarów. Trzeba to zrobić w taki sposób, by z opisu (obiektywność, kompletność i szczegółowość – to cechy podstawowe dla tej części opracowania) jednoznacznie wynikał wniosek i ocena.

Jeżeli poprzednie części audytu zostały opracowane wnikliwie precyzyjnie, kompletnie oraz z dbałością o szczegóły, to przedmiotowa część nie powinna sprawić Wykonawcy zbytnich problemów, choć jak to w życiu, różnie to bywa...

Podstawowe obszary, jakimi zazwyczaj audytor się zajmuje, to:

Analiza ruchu osobowego

Odwzorowanie ruchu osobowego na terenie obiektu i w jego najbliższym otoczeniu.

Ściśle opisuje się miejsca, przez które odbywa się ruch osób, nasilenie tego ruchu w zależności od miejsca (ciągu komunikacyjnego, poziomu obiektu, itp.) i czasu.

Opisuje się również profil osób poruszających się na terenie obiektu i w jego bezpośredniej bliskości.

Analiza ruchu pojazdów

Analogicznie do ruchu osobowego opisuje się ruch pojazdów i maszyn wraz z wszystkimi jego zależnościami. Należy położyć duży nacisk na przyczyny, przebieg oraz celowość opisywanego ruchu oraz ich podział. Warto napomknąć również o bramach, kodyfikacji ruchu, polityce parkingowej.

Jeżeli ruch kolejowy nie jest zbyt mocno rozbudowany, jego opis można zawrzeć w tej części. Przy dużym stopniu komplikacji zalecane jest stworzenie odrębnego podrozdziału.

Ruch materiałowy

Zasada „*idź za pieniądzem lub za człowiekiem*” sprawdza się w tej pracy zawsze. W moim rozumieniu „*pieniądz*” to zarówno informacja, towar, produkt, dokument i inne dobra niosące za sobą wartości, a „*człowiek*” jest rozumiany jako zagrożenie (zawsze rozważane jako potencjalnie umyślne i celowe).

Opis, stan techniczny oraz analiza funkcjonalna istniejących systemów ochrony technicznej

- systemy zabezpieczeń: CCTV, SKD, SWiN, Ppoż.
- bariery (i podziały) architektoniczne i administracyjne
- systemy oświetlenia i doświetlenia

System ochrony fizycznej

- Centrum Decyzyjne i Zarządzania Ochroną – tzw. Monitoring
- zabezpieczenie proceduralne (instrukcje, rozporządzenia i procedury wewnętrzne Organizacji)
- polityka bezpieczeństwa, zarządzanie kryzysem i utrzymanie ciągłości działania
- dokumentacja operacyjna (Plan/Instrukcja Ochrony, procedury wykonawcze)
- podział na strefy ochronne oraz stopień ich zabezpieczenia
- analiza funkcjonującego systemu ochrony fizycznej
- ocena jakości usługi ochrony fizycznej
- ocena funkcjonalna systemu ochrony fizycznej

Podsumowanie

Element opracowania będący kwintesencją i streszczeniem wszystkich poprzednich części. Przeznaczony do przedstawienia podczas prezentowania i streszczenia wyników audytu oraz przekazywania materiału w ręce Zleceniodawcy.

„Czego NIE robić i dlaczego?”, czyli ostrzeżenia, zasady i najczęstsze wpadki

Wiele jest rzeczy, których podczas realizacji robić nie wolno, nie powinno się i nie wypada. Z informacji jakie posiada autor wynika, że najczęstsze „wpadki”, jakie zaliczają audytorzy, to

Audyt „pod ustalony efekt”

Taka sytuacja ma miejsce, gdy – z różnych przyczyn, jednak rzadko znacznych – Wykonawca audytu, jeszcze przed rozpoczęciem swojej pracy na Obiekcie zna już jego efekt końcowy. Zawarte w nim diagnozy, zalecenia i oceny poszczególnych procesów i obszarów są tendencyjne, naciągane i tak sformułowane, by pokazywały rzeczywistość taką, na jakiej zależy... właśnie, komu na tym może zależeć? Z obserwacji autora artykułu wynika, że praktycznie każdemu (choć z reguły są to wzajemnie zaprzeczające sobie cele).

Wszyscy mogą być osobiście zainteresowani by pokazać określoną „prawdę” w określonym kontekście. Zdaniem autora artykułu, nie ma gorszego podejścia do audytu, jeżeli jeszcze można wtedy o audycie mówić.

Zlekceważenie Organizacji/Obiektu

Rzadko można się spotkać z takim podejściem, lecz niestety można. Widać wyraźnie tok myślenia audytora „przecież zrobiłem już milion audytów takich obiektów, po co więc się męczyć – „wiem już wszystko”. Nie muszę się przyglądać, badać, zbierać informacji, prowokować i przeprowadzać wywiadów...

Jaki jest efekt? Absolutnie nie przystający do audytowanej Organizacji. Błędy w danych wyjściowych powodują „rozchwianie” sum częściowych, a co za tym idzie – ocen i wniosków pokontrolnych. Plany naprawcze (zalecenia) będą nietrafione, a z czasem powodujące więcej szkody niż pożytku.

Przyjęte z góry założenia

Przyjęcie (i tu o dziwo, takie podejście częściej zdarza się wśród Zleceniodaw-

ców niż Wykonawców), że pewne procesy i zależności są oczywiste i nie wymagają zgłębiania, powoduje podobny efekt, do opisanego powyżej.

Narzucone „oczywistości” mogą, ale nie muszą być poprawnie przedstawione. Audytor nie może i nie powinien opierać się na tak przedstawionych danych, bo wówczas bierze pełną odpowiedzialność za źle sformułowane i nietrafione oceny i wnioski.

Źłe oceny zagrożenia

W pierwszej części opracowania, stosunkowo łatwo jest źle ocenić możliwość wystąpienia zagrożenia lub zagrożeń i jego/ich skutki.

Tak może się stać, gdy audytor tworzy opracowanie równoległe z prowadzeniem badań na terenie Obiektu. Taki sposób prowadzenia pracy posiada swoje zalety, ale należy wtedy bardzo uważać na przedwczesne wnioski i oceny.

Nieprawidłowe wnioski i oceny pokontrolne

Tego czasem nie da się uniknąć... Jest to zależne nie tylko od szczegółowości, obiektywności, dokładności etc., itp., badań i całego opracowania, ale też od merytorycznej wartości i doświadczenia audytora. Jednak najczęściej zdarza się to, po ... (Ustawa z dnia 7 października 1999 r. o języku polskim, która narzuca obowiązek przeciwdziałania jego wulgaryzacji) „niedopracowanej” części badawczej audytu.

Czasem nie da się też uniknąć po prostu błędu. Zbyt duża pewność siebie, nadinterpretacja, niedoszacowanie i/lub przeszacowanie czegoś, nie zauważenie jakiejś zależności, brak powzięcia jakiejś części wiedzy – przyczyn może być mnóstwo, a skutek jest ważny... po prostu popełniamy błąd.

„Zawalony” Plan Naprawczy

Wszystkie przyczyny są takie same, jak w powyżej wymienionej części, dot. wniosków i ocen pokontrolnych.

Jak się wywiązać z nietrafionych deklaracji i zbyt wczesnie wyciągniętych wniosków?

Przyznać się do błędu.

To proste i oczywiste, jednak nader rzadko stosowane w praktyce. Nie tylko audytorzy, ale generalnie duża część ludzi potrafi tak zagmatwać, zakręcić i poszukać wydumanych usprawiedliwień, byle

tylko nie przyznać: „pomyliłem się”. Takie proste i nieskomplikowane...

Na szczęście, w mojej pracy zdarzyć się to może tylko wtedy, gdy trzeba oddać opracowanie w częściach (unikam jak ognia), lub gdy lekce sobie zważę dane zagadnienie. Niestety zdarzyło się kilka razy i... bolało, gdy trzeba było potem powiedzieć „Przepraszam, pomyliłem się” brrrr...

Przebieg audytu?

Pisałem już „Co zrobić, żeby zrobić”, a teraz jest pora, żeby napisać „JAK to zrobić”. Nie o wszystkim napiszę, a nawet – proszę o wybaczenie, ale cenię sobie swoją wiedzę i jej (tak sobie przynajmniej wmawiam) unikatowość – niewiele tu napiszę.

Dobór odpowiednich narzędzi, jest pierwszą rzeczą, o którą trzeba zadbać.

Dla audytora nie ma lepszego narzędzia niż wizje lokalne, obecność na terenie audytowanego obiektu, własne obserwacje, zadawanie pytań, wywiady, etc., czyli zbieranie danych/informacji.

Praca na zebranych danych, to powinien być następny krok.

Mając zebrane już informacje, dokonujemy pracy porównawczej, a posiadamy do niej wzorce, w postaci:

- kodyfikacji zasad i form (w tym wypadku) bezpieczeństwa i ochrony
- norm branżowych
- dobrych praktyk branżowych
- wewnętrznych regulacji Organizacji audytowanej (przyjętych polityk, procedur, etc.)
- metodyk

Właściwie (to znaczy – najczęściej jak się da) do nich sięgając i korzystając, można osiągnąć bardzo wiele. Zwłaszcza, jeżeli jednym z zadań przed nami stojących jest zakres, jaki został ostatnio postawiony przed autorem artykułu:

1. *Weryfikacja Planu Ochrony. W przypadku, gdy z wniosków będzie wynikała celowość modyfikacji planu, Wykonawca zapewni wsparcie merytoryczne w uzgodnieniu nowej wersji przedmiotowego dokumentu;*
2. *Przegląd procedur związanych z kontrolą ruchu (towarowego i osobowego) na bramach;*
3. *Przegląd procedur związanych z reestracją i kontrolą czasu pracy pracowników ochrony;*
4. *Przegląd procedur związanych z reestracją pracowników i sprzętu firm zewnętrznych na terenie Obiektu;*

5. *Zgodność zakładowych regulaminów, instrukcji i procedur z instrukcjami i procedurami ochrony pod kątem spójności zadań wskazanych w tych dokumentach.*

Ten zakres, który powyżej wyszczególniono, wymagał pracy z pozyskaną (a czasem – zdobytą) informacją na dokumentach udostępnionych Wykonawcy. W tym miejscu leży odpowiedzialność Zleceniodawcy – nie można ograniczać Wykonawcy dostępu do dokumentów (czyli – danych) i oczekiwać wyczerpującego opracowania. Czy tylko Zleceniodawcy? To rozpatrzmy w dalszej części artykułu.

Gdy dane są zebrane, przepracowane, czyli porobiono już różne zestawienia, statystyki, tabele i oceny, należy wprząc własną (lub zapożyczoną) metodykę postępowania. Niejednokrotnie warto zastosować normę PN-ISO 31000:2012 „Zarządzanie ryzykiem – Zasady i Wytyczne”, której zapisy stosować w wybranych obszarach za pomocą mieszanych technik zbierania danych i ocen ryzyka. Łączymy metody jakościowych i ilościowych. Możemy również stosować metody opisane w normie ISO/IEC 31010:2009 „Risk management – Risk assessment techniques”, przede wszystkim w zakresie analizy konsekwencji poszczególnych ryzyk, a także efektywności zabezpieczeń.

Oceny, opisy, zalecenia pokontrolne

Wynikiem pracy na zebranych danych, powinny być wszelkiej maści oceny. Zagrożeń, stanu zabezpieczeń (tabela oceny zagrożeń, tabela audytu bezpieczeństwa Obiektu), jakości, funkcjonalności i pozostałych zakresów mieszczących się w ramach audytu.

Moja rada – przyłóżcie się. Jeżeli sami będziecie robić audyt, to od nakładu włożonej pracy zależy jakość opisu i wytłumaczenie proponowanych zmian – czytając zaleceń. Lepiej tu napisać o dwa zdania więcej, dobrze wyjaśniając np. zależności w procesach audytowanej Organizacji, niż oszczędzając miejsca założyć, że Zleceniodawca jest w pełni świadom uwarunkowań mających wpływ na bezpieczeństwo jego Organizacji.

Jak unikać wpadek

Nie ma na to gotowej recepty, a raczej możliwości zabezpieczenia jest tyle, że same w sobie mogą być tematem na artykuł. Niezależnie od przyjętej strategii unikania wpadek, zawsze warto dotożyć starań, żeby dobrze i jak najbardziej precyzyjnie określić:

Zakres audytu/opracowania

To daje nam możliwość ograniczenia opracowania do obszarów, do których się zobligowaliśmy jako audytor. Jednak przy każdym praktycznie audycie Wykonawca widzi rzecz/proces, który ma pośredni lub bezpośredni wpływ na bezpieczeństwo Organizacji, a nie leży w zakresie audytu. I co wtedy? Czy pominąć milczeniem? Niby można, ale jakoś to stoi w sprzeczności z etyką zawodową.

Zawsze wtedy można dopisać część, zatytułowaną „Spostrzeżenia spoza zakresu opracowania” i nie dość, że łapiemy dodatkowe punkty u Klienta, to jeszcze dopełniamy opracowanie.

Wyłączenia

Wyszczególnione wyłączenia pozwalają na wyłączenie specyficznych procesów, uwarunkowań, co do których posiadliśmy wiedzę, że nie powinny, lub z powodu decyzji Klienta, lub innych względów nie będą audytowane.

Przykład:

Z zakresu opracowania wyłącza się cały obszar zarządzania kryzysem, utrzymania ciągłości działania i bezpieczeństwa technologicznego produkcji.

I mamy temat z głowy – nikt nie może nam zarzucić, że pominęliśmy obszary, które bardzo luźno są związane z bezpieczeństwem fizycznym, na którym się koncentrujemy.

Zastrzeżenia

To samo dotyczy zastrzeżeń. Dla własnego bezpieczeństwa warto zapisać każde zastrzeżenie, które może mieć wpływ na jakość i zawartość merytoryczną opracowania.

Poniżej zamieszcza się przykładowe, zaczerpnięte z audytu jednej z polskich hut zapisy, dotyczące uwag, wyłączeń i zastrzeżeń.

„Opracowanie ma zdefiniować (...) ze wskazaniem miejsc, instalacji, urządzeń i obszarów podatnych na wybrane zagrożenia oraz pokazać (...), ze szczególnym uwzględnieniem roli oraz zadań ochrony fizycznej, funkcjonalności zabezpieczeń technicznych (...). Ocenie podlegają:

1. *System ochrony fizycznej;*
2. *Bezpieczeństwo stref wejścia/wyjścia oraz wjazdu/wyjazdu;*

3. Bezpieczeństwo punktów newralgicznych dla utrzymania ciągłości produkcji;
4. Funkcjonalność mechanicznych i elektronicznych systemów zabezpieczeń;
5. Dokumentacja operacyjna Ochrony – Plany Ochrony i inne udostępnione dokumenty;
6. Dokumentacja wewnętrzna Zamawiającego.

Ze względu na charakter opracowania, z zawartości wyłącza się następujące obszary:

1. Bezpieczeństwo przeciwpożarowe;
 2. Bezpieczeństwo teleinformatyczne;
 3. Bezpieczeństwo informacji: wrażliwych, osobowych, niejawnych i tajemnice Organizacji;
 4. Obszar strat, identyfikacja ich przyczyn, zakres oraz wielkość fraudów;
 5. Zarządzanie kryzysem i podejmowanie działań antykryzysowych;
 6. Funkcjonowanie obiektów w sytuacji potencjalnie skutkującej zniszczeniem substancji obiektu i przerwania jego działania – w czasie zagrożenia zewnętrznego i w czasie wojny.
- Ze względu na kompetencje Wykonawców, nie określa się w niniejszym dokumencie zalecanych

rozwiązań technologicznych i produkcyjnych z zakresu utrzymania ciągłości produkcji.

Czyni się zastrzeżenie, że wnioski pokontrolne mogą być obciążone błędem, wynikającym z:

1. Przekazania błędnych i/lub niepełnych danych Wykonawcy podczas wywiadów;
2. Przygotowania poszczególnych Zakładów Organizacji do współpracy przy audycie;
3. Określonego poziomu ogólności opracowania;
4. Ograniczeń w dostępie do dokumentacji wewnętrznej Organizacji;
5. Ograniczenia dostępu do procesów mających wpływ na bezpieczeństwo Zakładów Organizacji, wynikających m.in. z przepisów BHP ograniczających swobodny dostęp do wszystkich obszarów wewnętrznych Organizacji oraz braku uprawnień audytorów (np. elektrycznych, kolejowych, gazowych, etc.).

Podsumowanie

Podsumowując wszystko powyższe można by powiedzieć, że całość opracowania, to dobro intelektualne audytora.

I coś w tym jest, bo zarówno przyjęta metodologia, sposoby gromadzenia danych i informacji, metoda budowania relacji interpersonalnych (niesamowicie wiele można wygrać, gdy się zbuduje właściwie), ale też sposoby i algorytmy wykorzystania wszystkiego, co zostało zgromadzone, świadczy o Wykonawcy.

Do tego wszystkiego dochodzi się latami, budując na kanwie poznanej na różnych szkoleniach, kursach i w szkołach teorii, swoją pracę – wartość dodaną, którą jest przemodelowanie teorii, dopasowanie do charakteru Wykonawcy, do metod jego pracy i jego podejścia do tej pracy. A która tak naprawdę odróżnia wyrobniaka od fachowca.

Krzysztof Moszyński

absolwent Wojskowej Akademii Technicznej i Akademii Obrony Narodowej, niespełniony doktorant AON. W branży ochrony od ponad 20 lat, od ponad 15 lat zajmujący się analizami i audytami bezpieczeństwa, pracujący w korporacjach międzynarodowych (Falck, Group4, Group4Securicor, a obecnie Seris Konsalnet), odpowiedzialny za konsulting, doradztwo (audyty) i konfigurację nowych systemów bezpieczeństwa u najbardziej nawet skomplikowanych strukturalnie Organizacjach. Autor ponad 500 specjalistycznych opracowań eksperckich, wykonawca ponad 200 audytów systemów ochrony, zabezpieczeń i bezpieczeństwa dla Organizacji z wszystkich branż, autor kilkunastu publikacji. Związany pasją i zainteresowaniami z branżą ochrony i zabezpieczenia.

Reklama



Kolejne edycje Konferencji
SECURITECH i SECURITECH & DEFENSE
 w 2020 roku

Szczegóły w numerze 1/2020

NOWY SAMOCHÓD W FIRMIE? JAK GO SFINANSOWAĆ?

Jeszcze dwie dekady temu polskie przedsiębiorstwa nabywały samochody przede wszystkim z własnych środków, ewentualnie korzystały z kredytów przeznaczonych na ten cel. Jednak obecnie istnieją inne sposoby finansowania zakupu samochodów, które powinien znać każdy właściciel firmy.

Zakup samochodów za gotówkę

Firmy z sektora MŚP, które decydują się na **zakup nowego auta za gotówkę** muszą liczyć się z faktem, iż taka inwestycja zamraża znaczne środki finansowe. Co prawda, przedsiębiorcy w ten sposób nie narażają się na dodatkowe koszty związane na przykład z koniecznością opłacania oprocentowanych rat kredytu, ale muszą się liczyć z ograniczeniem środków, które mogłyby zostać przeznaczone na inwestycje czy rozwój firmy.

Za decyzją **pozyskania samochodu** bez kredytu czy leasingu przemawia jednak brak wielu formalności, koniecznych do spełnienia w przypadku innych form finansowania. Nie bez znaczenia jest również fakt, iż samochód wówczas od początku stanowi własność firmy, zatem

w sytuacji wystąpienia problemów z płynnością finansową nie ma zagrożenia, iż auto zostanie firmie odebrane, z powodu niewywiązywania się ze zobowiązań.

Outsourcingowe modele finansowania

Coraz więcej firm z sektora MŚP korzysta z **outsourcingowych modeli finansowania samochodów**, a zainteresowanie tymi sposobami nieustannie się zwiększa. Do takich form finansowania należy **leasing** oraz **wynajem długoterminowy**. Warto jednak mieć na względzie, iż obie formy finansowania, chociaż nierzadko mylone, dzieli jednak wiele różnic.

Leasing to połączenie elementów kredytu i dzierżawy, a więc przedsiębiorca może korzystać z pojazdu na warunkach,

jakie zostają określone w **umowie leasingowej**. W tym wypadku jednak auto nie jest jego własnością. Przedsiębiorstwa, które decydują się na **leasing samochodu**, również stają przed wyborem dwóch jego rodzajów, a mianowicie **leasingu operacyjnego i finansowego**.

Leasing finansowy to rodzaj leasingu, w jakim **przedmiot leasingu** staje się częścią majątku przedsiębiorstwa, które z tego instrumentu korzysta. W takim wypadku pojazd jest od początku **umowy leasingu** składnikiem majątku firmy, a raty mogą być dostosowane do wymagań oraz możliwości budżetowych przedsiębiorstwa. Jednak w tym wypadku od razu, niejako z góry, firma musi **zapłacić podatek VAT** za samochód, a rat kapitałowych nie może wliczyć w koszty. Korzystająca z takiej **umowy leasingowej** firma ponosi również pewne ryzyko rzeczowe oraz cenowe, zobowiązując się do wnoszenia opłat nawet w przypadku, gdy samochód zostanie na przykład skradziony. W leasingu finansowym pewnego rodzaju rekompensatę za większe miesięczne raty stanowi jednak **możliwość wykupu samochodu po cenie zdecydowanie niższej**, aniżeli jego **wartość rynkowa**.

Z kolei **leasing operacyjny** daje przedsiębiorstwu możliwość **zaliczenia do kosztów uzyskania przychodu** prawie wszystkich **wydatków**, jakie wiąże się z użytkowaniem pojazdu. Będzie to zatem **rata leasingowa**, opłata wnoszona na początku, czyli tak zwany **czynsz inicjalny**, a także wszelkie wydatki za paliwo, przeglądy czy zakup wyposażenia. W **leasingu operacyjnym** podatek VAT jest **naliczany stopniowo**, przy każdej racie. Kolejną zaletą **leasingu operacyjnego** jest **niższa**, aniżeli w przypadku leasingu finansowego, **miesięczna rata za użytkowanie auta**, ponieważ przez czas **leasingu** splanowana jest jedynie **utrata wartości samochodu**. W efekcie **cena wykupu** stanowi **realną wartość auta z chwilą wygaśnięcia umowy**. Warto zaznaczyć, że **zakup samochodu nie jest obligatoryjny**, a firma może podpisać umowę na użytkowanie nowych samochodów, nie mierząc się z koniecznością sprzedaży



starszych, użytkowany dotychczas modeli. Ten rodzaj leasingu, zwany także **leasingiem z rynkową wartością końcową**, umożliwia płać niskich rat, które wynikają jedynie z utraty wartości samochodu w czasie, kiedy firma z niego korzysta. **Umowy tego rodzaju są zawierane na okres od 2 do 4 lat.** To interesująca opcja, ponieważ po upływie czasu, jaki został oznaczony w umowie, przedsiębiorca może **wymienić auto na nowe**, zwracając stary samochód.

Wynajem długoterminowy stanowi umowę leasingu, jaka jest zawierana na czas **od 2 do 5 lat zazwyczaj bez możliwości wykupu**, a także z **serwisem samochodu i jego ubezpieczeniem**, zawierającym się **w cenie raty miesięcznej**. Wynajem obejmuje więc nie tylko finansowanie pojazdów, lecz zarazem pełen zakres usług zarządzania samochodami, a więc outsourcing floty przedsiębiorstwa. W zakresie miesięcznych rat mieszczą się zatem usługi dodatkowe, jak serwisowanie i naprawy mechaniczne, zakup oraz przechowywanie i wymiana opon, usługi *assistance*, a także samochód zastępczy, ubezpieczenia oraz likwidacja szkód. Wybór tej opcji pozwala przedsiębiorstwu



zredukować do minimum czynności, które wiążą się z obsługą floty firmowej.

Jaki sposób jest najkorzystniejszy dla przedsiębiorstwa?

Podjęcie decyzji dotyczącej **sposobu wejścia w posiadanie nowych samochodów** jest dla firmy kluczowe pod względem finansowym, organizacyjnym, logistycznym. Dlatego firmy z sektora MŚP często podejmują takie decyzje po **konsultacjach z profesjonalistą** zajmującym się **optymalizacją kosztów zarządzania flotą** pojazdów.

Takie usługi oferują niektóre sieci dealerskie, jak na przykład **Grupa AUTO WIMAR**, oddająca do dyspozycji **klientów**

z sektora MŚP – usługę Biznes Ekspert, która realizuje usługi doradcze w zakresie obsługi i zarządzania flotą, w ramach których wskazuje optymalne rozwiązania m.in. w zakresie zakupu nowych aut, ich serwisowania czy sprzedaży. **Doradcy**, bazując na swoim **doświadczeniu** oraz **znajomości praw** rządzących rynkiem samochodowym, w **indywidualny sposób** określają potrzeby danej firmy, a także dopasują ofertę, która na nie najlepiej odpowiada. Przedsiębiorstwo może wówczas skupić się na zarządzaniu rozwojem, pozyskiwaniu nowych rynków i rozwijaniu działalności, wiedząc, że flota i sprawy z nią związane znajdują się pod dobrą opieką.

Reklama



GRUPA AUTO WIMAR
Twój Serwis i partner marki SKODA

WSPARCIE DORADCY
dobór auta, wyposażenia, opcji finansowania

FINANSOWANIE
gotówka, leasing lub wynajem

TELEMATYKA
zdalna kontrola kosztów i bezpieczeństwa

 skoda-biznesekspert.pl  22 5106666

 **ŠKODA**





**BIZNES
EKSPERT**

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 drukowana: 60 zł elektroniczna: bezpłatna
- Dwuletnia drukowana: 110 zł elektroniczna: bezpłatna
- Studencka drukowana: 40 zł elektroniczna: bezpłatna

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

**BEZPŁATNA PRENUMERATA ELEKTRONICZNA
DO POBRANIA NA STRONIE**

www.ochrona-bezpieczenstwo.pl



Lubię to!

**Wejdź na nasz
profil i polub nas!**

www.facebook.com/ochronaibezpieczenstwo



**Dwumiesięcznik powstaje
we współpracy z:**



alarmy.org

Kontakt



**OCHRONA
i BEZPIECZENSTWO**
OBIEKTÓW I BIZNESU

Rok XXII nr 1/2020 (148)

www.ochrona-bezpieczenstwo.pl

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

Wydawca:

Mediafachowe, ul. Rosoła 10a
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. Rosoła 10a, 02-786 Warszawa
redakcja@ochrona-bezpieczenstwo.pl
www.ochrona-bezpieczenstwo.pl



Robert Mościcki

Redaktor Naczelny
tel. 606 911 071
r.moscicki@ochrona-bezpieczenstwo.pl



Lidia Tuchowska

Redaktor/Marketing iPR
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: Tomasz Aleksandrowicz, Tomasz Balcerzak, Edmund Basatyga, Grzegorz Cieślak, Jerzy Ciszewski, Michał Czuma, Andrzej Dubrawski, Robert Gabrysiak, Urszula Garlińska, Sebastian Hładun, Maciej Korczak, Michał Kozłowski, Waldemar Kubik, Krzysztof Łangowski, Dobrosław Mąka, Cezary Mecwaldowski, Adam Radomyski, Jarosław Stelmach, Ewa Sobór, Krzysztof Młudzik, Krzysztof Moszyński, Robert Poklek, Jerzy Taczalski, Dariusz Woźniak, Damian Żabicki.

Zdjęcia: zespół redakcyjny, materiały promocyjne, www.fotolia.com

Łamanie i opracowanie graficzne: Ważka Łukasz Piotrowski

Druk: Art.-Druk w Kobylce

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 opiniami Autorów.

SAS-Hitech-Xpose to ręczny, kompaktowy, miernik gęstości zaprojektowany dla służb porządku publicznego do detekcji ukrytych przemycanych przedmiotów. Cechuje się niską wagą, wzmacnianą obudową odporną na uszkodzenia i warunki atmosferyczne.

Bardzo często przemyt odbywa się w ukrytych, trudno dostępnych przestrzeniach takich jak opony, grodzie, puste przestrzenie w pojeździe lub łodzi, tam gdzie bezpośrednia obserwacja nie jest możliwa bez czasochłonnego demontażu, a nierzadko trwałego uszkodzenia sprawdzanego obiektu.

SAS-Hitech-Xpose jest w stanie wskazać obecność nielegalnie przewożonych przedmiotów ukrytych w takich miejscach. Urządzenie działa na podstawie pomiaru zmian gęstości na sprawdzanym obszarze. Niespodziewane zmiany wskazują na obecność ukrytych przedmiotów lub komór.



Najważniejsze cechy:

- Krótszy czas reakcji i poprawione właściwości penetracji dzięki dużemu detektorowi
- Ekran LCD 2,5" wyświetlający wykres zależności gęstości od czasu
- Ergonomiczna konstrukcja pozwalająca na obsługę jedną ręką
- Podłączenie USB lub bezprzewodowe dla zewnętrznego wyświetlacza
- Gniazdo słuchawek 3.5mm pozwalające na pracę w głośnym otoczeniu, lub w ukryciu przed osobami postronnymi
- Wzmocniona konstrukcja dla użytkowania w środowisku przemysłowym i w terenie
- Lekka i kompaktowa budowa
- Wbudowany test

• Specyfikacja

Źródło promieniowania:	Bar 133 (nie przekracza 10 μ Ci, 370kBq)
Ochrona źródła:	stop wolframu z przesłoną sprężynową, zamykaną w razie awarii.
Moduł wykrywacza:	CsI (TI), jodek ceszu aktywowany talem
Głębokość penetracji:	15,2cm
Szybkość skanowania:	0,25 sekundy/odczyt
Tryby pracy:	Survey: wskazywanie obecności źródeł promieniowania w otoczeniu urządzenia Inspect: badanie powierzchni i informowanie o niespodziewanych zmianach gęstości Kalibracja Wbudowany test
Wyświetlacz:	graficzny LCD, 400 x 240, wskaźnik niskiego stanu baterii
Alarm dźwiękowy:	60dB, 2,4 kHz, 0,5 s, automatyczne dostosowanie wartości wyzwalającej alarm do 1 odchylenia standardowego, odczyt rosnący: impulsy 50 dB co 0,5 sekundy
Zasilanie:	2 x bateria alkaliczne AA
Czas pracy:	do 40 godzin ciągłej pracy do 6 miesięcy w stanie czuwania

• SAS-Hitech-Xpose – charakterystyka promieniowania

Operator otwiera i zamyka źródło promieniowania za pomocą dwóch przycisków położonych po obu stronach urządzenia, których jednoczesne wciśnięcie obraca osłonę. Zwolnienie któregośkolwiek z przycisków powoduje obrót osłony do pozycji zamkniętej, w której pozostanie do czasu kolejnego użycia.

Dawka promieniowania odbierana przez operatora lub osobę postronną wynosi poniżej 0.05 mR/h (dla całego ciała). Poniżej przedstawiono rezultat niezależnie przeprowadzonego pomiaru dawki. Zaobserwowana dawka pochodząca z urządzenia Xpose wynosi od 0.01 mR/h do 0.03 mR/h, zarówno przy otwartej jak i zamkniętej osłonie źródła promieniowania.

Portfolio produktów Hytera Ad Hoc Rozwiązania dla Łączności Kryzysowej

—— Szybkie uruchomienie, Bezpieczne i Niezawodne



Mobilna
Brama Dostępowa
E-PRAD(G)



Przełącznik
Ad Hoc DMR
E-pole100



Mobilne
System Dyspozytorskie
E-center



Mobilny
Przełącznik Ad Hoc DMR
E-pole100



Mobilny Przełącznik
i Brama Dostępowa
GTW-836C

Autoryzowany Partner: