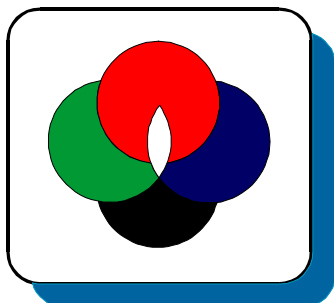




Ogólnopolskie Stowarzyszenie Inżynierów i Techników
Zabezpieczeń Technicznych
i Zarządzania Bezpieczeństwem
„POLALARM”

ul. Nowogrodzka 18 lok. 8

00-511 Warszawa

www.polalarm.org

Konto bankowe: ALIOR BANK S.A. NRB 70 2490 0005 0000 4520 4686 4115

tel./fax: 22 626 90 31

22 625 57 43

e-mail: polalarm@polalarm.com.pl

Członek Federacji
Stowarzyszeń
Naukowo-Technicznych



BIULETYN INFORMACYJNY

ISSN 1731-62-78

KWARTALNIK Nr 4 / 2015

Ogólnopolskiego Stowarzyszenia Inżynierów i Techników
Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem
„POLALARM”



**Z okazji Świąt Bożego Narodzenia
oraz Nowego 2016 Roku
najserdeczniejsze życzenia zdrowia,
wszelkiej pomyślności w życiu osobistym
i sukcesów w pracy zawodowej
życzy
Zarząd POLALARM**



W numerze:

- Zmiany w Zarządzie POLALARM
- Polski Mistrz Techniki Alarmowej 2016
- Stopnie zabezpieczenia i pojęcie ryzyka w nowych Normach „Systemy dozoru wizyjnego stosowane w zabezpieczeniach” i „Elektroniczne systemy kontroli dostępu” - dr inż. Andrzej Ryczer
- Przegląd prasy branżowej – Andrzej Walczyk
- SECUREX 2016
- Nowe prawo dla stowarzyszeń
- Usługi ochrony osób i mienia - koncesje
- XIII Forum Inżynierskie
- III Światowy Zjazd Techników Polskich
- FLIR Systems | Nowe kamery termowizyjne FLIR Vue™ dedykowane do dronów
- Zasada *in dubio pro tributario* nie może być "martwym" przepisem
- Pierwsza runda Alpol Bowling CUP za nami
- Targi, wystawy, Konferencje

Redaktor Naczelny: Artur Bogusz
Kolegium Redakcyjne:
Andrzej Wójcik, Andrzej Ryczer, Bożena Gozdowska
Siedziba „POLALARM”:
ul. Nowogrodzka 18 lok. 8, 00-511 Warszawa
tel./fax 22 626 90 31, 22 625 57 43
e-mail: polalarm@polalarm.com.pl, www.polalarm.org
Redakcja nie odpowiada za treść reklam i ogłoszeń.
Wszelkie prawa zastrzeżone.
Nakład jednorazowy 150 egz.

Warszawa

grudzień

2015 r.

Uprzejmie prosimy Członków Stowarzyszenia „POLALARM”

o zgłaszanie
na adres Biura Zarządu –
polalarm@polalarm.com.pl
tel. 22 626 90 31, 22 625 57 43

zmian:

- adresu do korespondencji
- adresu e-mail
- numerów telefonów

Zmiany Zarządzie „POLALARM”

W związku z rezygnacją z członkostwa w Stowarzyszeniu dotychczasowego Sekretarza Generalnego, Zarząd powierzył tę funkcję **kol. Andrzejowi Wójcikowi**, który do końca kadencji będzie łączył funkcję Wiceprezesa i Sekretarza Generalnego Zarządu.

POLSKI MISTRZ TECHNIKI ALARMOWEJ 2016

Stowarzyszenie „POLALARM” zaprasza producentów oraz dystrybutorów elektronicznych i elektromechanicznych urządzeń oraz systemów przeznaczonych do ochrony osób i mienia, do udziału w XVI edycji Konkursu

POLSKI MISTRZ TECHNIKI ALARMOWEJ 2016 im. Włodzimierza Kuczkowskiego.

Termin zgłoszeń upływa 31 stycznia 2016 r.

REGULAMIN KONKURSU

Komisja Konkursowa dokonuje oceny wyrobów zgłoszonych do Konkursu. Komisja nie rozpatruje praw własności i praw autorskich posiadanych przez Firmy do wyrobów zgłaszanych do Konkursu.

1. Konkurs jest organizowany przez Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM”, członka Federacji Stowarzyszeń Naukowo-Technicznych NOT.
2. Konkurs Stowarzyszenia „POLALARM”, zwany dalej Konkursem ma na celu:
 - a) promocję nowoczesnej myśli technicznej;
 - b) podkreślenie rangi i znaczenia postępu naukowo-technicznego w dziedzinie ochrony mienia;
 - c) nagradzanie i wyróżnianie wybitnych rozwiązań.

3. Nagrody w Konkursie są przyznawane za wybitne elektroniczne i elektromechaniczne urządzenia oraz systemy przeznaczone do technicznej ochrony mienia, a w szczególności: urządzenia systemów sygnalizacji włamania, napadu, pożaru, systemów telewizji dozorowej, kontroli dostępu, monitorowania zagrożeń, elektronicznego wyposażenia agentów ochrony fizycznej i zabezpieczeń pojazdów, transportu, ładunków.
4. Urządzenia i systemy do Konkursu mogą zgłaszać krajowi i zagraniczni twórcy i producenci oraz dystrybutorzy funkcjonujący w oparciu o polskie prawo gospodarcze.
5. Konkurs jest jednoetapowy i przeprowadzany na szczeblu ogólnokrajowym co dwa lata.
6. Komisja Konkursowa jest 11 osobowa, wybrana spośród członków Stowarzyszenia.
7. W pracach Komisji mogą brać udział powołani eksperci, bez prawa udziału w głosowaniu.
8. W Komisji Konkursowej nie mogą brać udziału zgłaszający urządzenia i systemy do Konkursu w danym roku kalendarzowym.
9. Wnioski o udział w Konkursie winny być składane na „Wniosku o udział w Konkursie Polski Mistrz Techniki Alarmowej”. W przypadku zgłoszenia dwóch identycznych wyrobów Komisja rozpatrywać będzie wniosek, który wpłynął jako pierwszy.
10. Z wnioskiem wskazane jest złożenie:
 - a) urządzenia lub systemu,
 - b) dokumentacji technicznej, rysunków, fotografii,
 - c) opinii recenzentów, instytutów, laboratoriów, oś rod-ków badawczo-rozwojowych firm projektowych i usługowych, użytkowników lub innych.
11. Dopuszcza się maksymalnie 10-minutową prezentację wyrobu przez Zgłaszającego przed członkami Komisji w terminie uzgodnionym z organizatorem Konkursu. W przypadku niemożności zaprezentowania wyrobu w siedzibie organizatora Konkursu lub na terenie Warszawy, Zgłaszający pokrywa koszty delegacji i dojazdu 2 członków Komisji do miejsca prezentacji
12. Konkurs będzie przeprowadzony w następujących kategoriach przedmiotowych:
 - I. Urządzenia i systemy sygnalizacji włamania i napadu
 - II. Urządzenia i systemy sygnalizacji pożaru
 - III. Urządzenia i systemy nadzoru telewizyjnego
 - IV. Urządzenia i systemy kontroli dostępu
 - V. Zintegrowane systemy sygnalizacji zagrożeń
 - VI. Urządzenia i systemy transmisji alarmu
 - VII. Systemy zabezpieczenia przeciwwkradzieżowe-go pojazdów oraz urządzenia i systemy zarządzania bezpieczeństwem transportu osób i ładunków
 - VIII. Inne innowacyjne urządzenia i techniczne systemy ochrony oraz wspomagające ochronę fizyczną
13. Za każde zgłoszone urządzenie lub system – Zgłaszający winien wnieść opłatę wpisową w wysokości 900 zł + obowiązująca stawka VAT (urządzenia

wchodzące w skład zgłoszonego systemu nie będą oceniane indywidualnie). Dla Członków Ogólnopolskiego Stowarzyszenia Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem „POLALARM” opłata wynosi 600 zł + obowiązująca stawka VAT. Zgłaszający wyrób do więcej niż jednej kategorii wnosi dodatkową opłatę w wysokości 30% w/w stawki za każdą dodatkową kategorię.

14. W każdej kategorii przedmiotowej zostanie wybrane jedno urządzenie lub system, które otrzyma tytuł „Polski Mistrz Techniki Alarmowej” i do trzech wyróżnień w każdej z kategorii.
15. Spośród urządzeń lub systemów nagrodzonych jako „Polski Mistrz Techniki Alarmowej” zostanie wyłoniony Zwycięzca Konkursu, któremu zostanie przyznana nagroda „Złota Zbroja”.
16. Ostateczny termin zgłoszeń upływa z dniem 31 stycznia 2016 r.
17. Przyznanie tytułów, nagród i wyróżnień w Konkursie Ogólnokrajowym nastąpi do dnia 3 marca 2016 r., natomiast zakończenie Konkursu i wręczenie nagród nastąpi na Międzynarodowej Wystawie SECUREX w Poznaniu.
18. Decyzje Komisji Konkursowej Stowarzyszenia „POLALARM” w zakresie przyznawania tytułów, nagród i wyróżnień w Konkursie są ostateczne.
19. Niniejszy Regulamin Konkursu wchodzi w życie z dniem zatwierdzenia przez Zarząd Stowarzyszenia „POLALARM”.

Regulamin zatwierdzony przez Zarząd w dniu 18 września 2013 r., zmiany w Regulaminie zatwierdzone przez Zarząd w dniu 17 czerwca 2015 r.

Stopnie zabezpieczenia i pojęcie ryzyka w nowych Normach „Systemy dozoru wizyjnego stosowane w zabezpieczeniach” i „Elektroniczne Systemy Kontroli dostępu”

W nowych normach Systemy Alarmowe dotyczących systemów dozoru wizyjnego stosowanych w zabezpieczeniach VSS¹ (*Video surveillance systems in security applications* – dawniej CCTV) oraz elektronicznych systemów kontroli dostępu EACS (*Electronic Access Control Systems* – dawniej kontroli dostępu) [1], [2], [3], [4], systemy i ich części składowe mają określony stopień zabezpieczenia (*security grade*). Cztery stopnie zabezpieczenia uwzględniają poziom ryzyka, zależny od prawdopodobieństwa wystąpienia zdarzenia w zabezpieczanym obszarze - obiekcie oraz od potencjalnej szkody (skutku).

W zależności od stopnia zabezpieczenia systemy VSS i EACS różnią się swoją funkcjonalnością związaną między innymi z ich podstawowymi cechami tj.: **zabezpieczenie przez sabotażem** elementów – urządzeń składowych i **ograniczenia dostępu** do sterowań funkcjami systemów. Stopień zabezpieczenia zależny jest od celu obserwacji

¹ W artykule stosujemy nowe skróty VSS i EACS tak jak w nowych normach IEC [2], [3] i [4].

(VSS) albo od metody rozpoznania użytkownika (EACS). Podobnie jak w przypadku systemów alarmowych sygnalizacji włamania i napadu w systemach VSS i EACS stosownie do oszacowanego ryzyka wyróżnia się cztery stopnie zabezpieczenia.

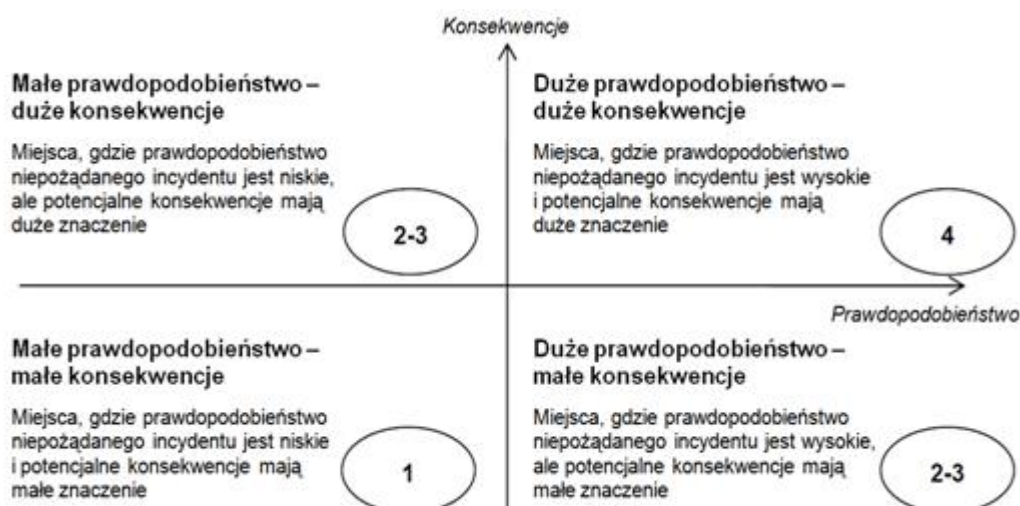
W systemach EACS stopień zabezpieczenia urządzenia jest określany przez klasyfikację cech funkcjonalnych np. tj.: monitorowanie stanu punktów kontroli dostępu, sygnalizacja stanu przymusu, powiadomienie za pomocą konsoli obsługi. Poziomy ryzyka określa się zależnie od wartości zabezpieczanych zasobów oraz od zamiarów (wiedzy/doświadczenia) i metod potencjalnego ataku osób mających zamiar obejść przejście kontrolowane.

W obiektach z zasobami o znacznej wartości, tj. obiekty: użyteczności publicznej, produkcji specjalnej, portowe morskie i lotnicze, banki, rafinerie, ze względu na szacowany poziom ryzyka są stosowane głównie systemy EACS stopni 3 i 4 przeznaczane do: zabezpieczania przed Sabotażem, atakiem terrorystycznym, dostępem do informacji poufnych, kradzieżą cennych zasobów itp.. Niżej będą

przedstawione wybrane problemy dotyczące stosowania systemów VSS i EACS, zwracając szczególną uwagę na podejście do szacowania ryzyka i na podstawowe cechy systemów decydujące o ich stopniu zabezpieczenia.

1. ZASADY OGÓLNE STOSOWANIA NORM SYSTEMY ALARMOWE – STOPNIE ZABEZPIECZENIA

Podstawowa zasada stosowania norm Systemy Alarmowe opiera się na doborze stopnia zabezpieczenia danego systemu do oszacowanego poziomu ryzyka, określono to w przypadku systemu VSS na rys.1, gdzie stopnie zabezpieczenia systemu – odpowiadające czterem ćwiartkom wykresu, oznaczono jako: 1, 2-3 i 4. Ryzyko uzależnia się od **konsekwencji** realizacji zdarzeń, obejmujących: obrażenia, utratę życia, uszkodzenia lub utratę mienia, utratę informacji i skażenia środowiska oraz od **prawdopodobieństwa** (możliwości) wystąpienia tych zdarzeń i dalszej ich realizacji zależnego np. od: sprawności służb ochrony, jakości ochrony fizycznej, pojawienia się zaburzeń społecznych i możliwości wystąpienie strat środowiskowych.



Rys. 1. Ryzyko i stopnie zabezpieczenia: 1, 2-3, 4 w odniesieniu do systemów VSS [1]

Wykres z rysunku 1, choć odnosi się ryzyka w środowisku stosowania systemów VSS bardzo dobrze ilustruje przyjęte w innych normach Systemy Alarmowe ogólne zasady stosowania dwóch pozostałych podstawowych systemów tj. sygnalizacji włamania i napadu oraz kontroli dostępu – choć tam ich stopnie zabezpieczenia określono w nieco odmienny sposób. W „najstarszej normie” [5] określono je w zależności od kwalifikacji/doświadczenia spodziewanych intruzów/włamywaczy i zakresu narzędzi z jakich będą korzystać, a w „normie nowszej” [3] zależnie od: wartości zasobów, znajomości systemów EACS, znajomości identyfikatorów i technologii IT oraz wartości środków przeznaczonych na realizację ataku, jak to zostanie wyjaśnione niżej.

2. KLASYFIKACJA STOPNI ZABEZPIECZENIA W SYSTEMACH VSS

Stopień zabezpieczenia systemu VSS, tak jak w pozostałych wymienionych wyżej systemów alarmowych zależy od **integralność systemu** oraz **integralność danych** przetwarzanych przez system. O integralności systemu decydują fizyczne zabezpieczenie elementów systemu (urządzeń i połączeń wzajemnych) oraz kontrola dostępu fizycznego i logicznego do urządzeń lub programowania

funkcji systemu. Celem zabezpieczenia (samego) systemu jest również sygnalizacja wszelkich awarii i ochrona przed umyślnym i niezamierzonym zakłócaniem pracy.

Na **integralność systemu** ma wpływ ochrona każdego elementu lub urządzenia systemu, jak również ochrona systemu VSS jako całości. Jeżeli stosowane są połączenia pomiędzy elementami systemu i interfejsy zewnętrzne do innych systemów alarmowych, to ich ochrona/monitorowanie stanowi również o integralności systemu VSS jak i o integralności systemu zintegrowanego.

Integralność danych polega na: identyfikacji (dokładna identyfikacja źródła danych, czasu, daty itd.); uwierzytelnieniu (zapobieganie modyfikacjom, usunięciom lub dodawaniu danych) oraz na ochronie danych (zapobieganie nieautoryzowanemu dostępowi do danych). Na integralność danych ma wpływ logiczny dostęp do danych i zapobieganie utracie lub manipulacji danymi.

Ze względu na różny zakres zadań w zakresie ochrony/dozoru realizowanych przez system VSS elementy, podsystemy i funkcje systemu mogą mieć **różne stopnie zabezpieczenia** w obrębie tego samego systemu – powinno być to wyraźnie określone w wymaganiach użytkowych.

Cztery stopnie zabezpieczenia systemów VSS określono (rys. 1) w zależności od poziomu oszacowanego ryzyka będącego funkcją **konsekwencji/skutków** np. tj: utrata życia, obrażenia, skażenia środowiska, uszkodzenia lub utrata mienia lub informacji. Stopnie są również funkcją **prawdopodobieństwa/możliwości** wystąpienia tych zdarzeń w miejscu - strefie obserwacji. Przykładowo, systemy 3 i 4 stopnia powinny być stosowane do ochrony zasobów w zakresie co najmniej od ryzyka średniego do wysokiego włącznie, jak niżej.

• Ryzyko w zakresie średnie do wysokiego (system VSS stopnia 3)

Dozór wizyjny obszarów o średnim do wysokiego poziomie ryzyka, system ma mieć wysoki poziom ochrony i wysoki poziom ograniczeń dostępu.

PRZYKŁAD: Duży magazyn zawierający produkty mało pożądane, zlokalizowany w obszarach o wysokim poziomie ryzyka tj. centra handlowe lub niewielkie magazyny (o powierzchni mniejszej niż 400m²) zawierające pożądane produkty o wysokiej wartości (np. produkty AGD, lekarstwa lub papierosy), zlokalizowane w obszarach o niskim poziomie ryzyka. Firmy usługowe o działalności związanej z dużymi wartościami, lecz bez poufnych informacji. Ochrona budynków użyteczności publicznej, portów, lotnisk, banków, rafinerii przed sabotażem lub atakiem terrorystycznym.

• Ryzyko wysokie (system VSS stopnia 4)

Dozór wizyjny obszarów o wysokim stopniu ryzyka, system ma mieć bardzo wysoki poziom ochrony i bardzo wysoki poziom ograniczeń dostępu.

PRZYKŁAD: Magazyny zawierające produkty wysoce pożądane (np. biżuteria, wysoce pożądane leki, telefony komórkowe lub papierosy), tj. centra handlowe zlokalizowane w obszarach o wysokim poziomie ryzyka. Firmy usługowe o działalności związanej z wartościami i poufnymi informacjami (np. laboratoria wojskowe, obiekty administracji państwowej - rządowe).

W normie [1] w 11 tablicach przedstawiono szczegółowo cechy funkcjonalne i parametry użytkowe systemów CCTV (gdzie jeszcze jest stosowany skrót CCTV, który w normie IEC [5] został zastąpiony przez VSS) w zależności od stopnia zabezpieczenia, w przypadku systemów stopni 3 i 4, wybrane ważniejsze parametry przedstawiają się następująco:

- przechowywanie – zapis danych (obrazów), czas reakcji: na sygnał wyzwalający zapis – maksymalnie 250ms, odtworzenia obrazu z pamięci – opóźnienie maksymalnie 2s,
- uwierzytelnienie każdego obrazu przy archiwizacji i wykonywanie kopii bezpieczeństwa, możliwości wykonania i weryfikacji kopii bezpieczeństwa,
- rejestrowanie zdarzeń systemowych, stanów systemu tj.: alarmy, sabotaże, utraty i odzyskania sygnałów, dane dotyczące źródła i czasu kopiowanych obrazów, logowanie, inne operacje dotyczące obrazów i zmian w konfiguracji systemu,
- monitorowanie połączeń – okresy monitorowania (stopień3/stopień4): 30s/10s z powiadomieniem 180s/30s,
- wykrywanie sabotażu – w urządzeniach: utrata sygnału, celowe zasłonięcie kamery, zastąpienie danych wi-

zyjnych w punkcie źródła sygnału i ograniczenie kontrastu (w systemach 4 stopnia),

- poziom dostępu – wykorzystuje się 4 klasyczne poziomy dostępu, w tym: zmiany konfiguracji, kodów dostępu, uruchomienie i zatrzymanie systemu – dozwolone tylko z poziomów 3 i 4 tzn. dla administratora (hasło/kod) i personelu serwisowego (jeśli dozwoli administrator); każda osoba i każdy użytkownik nie mają do tych poziomów dostępu.
- wymagania dotyczące kodów autoryzacji – liczba wariacji: klucz logiczny > 100 000, fizyczny > 15 000; dla systemu 4 stopnia klucz logiczny > 1 000 000, fizyczny > 50 000,
- dostęp do danych – możliwy z określonego poziomu dostępu, w tym eksportowanie i usuwanie danych – tylko z poziomu 3 i 4,
- dostęp do rejestrów systemu – z 3 i 4 poziomu dostępu, obejmujący: podgląd, eksportowanie i usuwanie rejestrów,
- dostęp do ustawień systemu – zmiany konfiguracji i ustawień tylko z poziomu 3 i 4,
- oznakowanie danych - obiekt, kamera, data, czas – od poziomu 2.

Należy wyraźnie zaznaczyć, że stopnie zabezpieczenia systemu VSS określone w normie – zależne od poziomu ryzyka, nie mają bezpośredniego związku z sześcioma celami stosowania systemów, które zostały określone w innej obszernej normie dotyczącej „zasad stosowania VSS” [2], takimi jak: **kontrola tłumy, detekcja intruza, obserwacja, rozpoznanie, identyfikacja i inspekcja**, gdzie np. określa się zalecany procent zajmowanej wysokości ekranu przez sylwetkę osoby/osób poddanych obserwacji – wynoszący od 5% do 400% wysokości ekranu, w zależności od określonego celu.

W zasadach stosowania zaleca się przed rozpoczęciem tworzenia projektu systemu przeprowadzenie oceny zagrożeń i analizy ryzyka w strefie obserwacji. Zagrożenia i ryzyka dotyczące danego miejsca powinny być zidentyfikowane i oszacowane ze względu na prawdopodobieństwo i skutki. W normach dotyczących zarządzania ryzykiem [6] i [7] opisano klasyczne zasady i przykłady prowadzenia analizy ryzyka, które mogą mieć zastosowanie również w precyzyjnym planowaniu systemów alarmowych.

W aspekcie ryzyka w procesie planowania i projektowania systemu VSS, należy rozważyć:

- wartość strat (wartość zasobów finansowych, niematerialnych w danej lokalizacji i wielkość skutków – przerw w działalności chronionego obiektu),
- lokalizację zasobów (jakość i zasięg istniejącej ochrony fizycznej, czy lokalizacja znajduje się w obszarze wysokiej przestępczości? czy panują niesprzyjające warunki środowiskowe?),
- zajętość (niezajętość lokalizacji przez użytkowników w dłuższym okresie czasu, obecność ochrony, dostęp publiczny),
- historię kradzieży, rabunków i zagrożeń w lokalizacji i jakie były metody ataku?

W tablicy 1 przedstawiono w przypadkach wybranych lokalizacji zalecane w zasadach stosowania VSS podstawowe cele i parametry systemu (liczba ramek/s, typ

kamery – PTZ). Cele te i parametry zależą od: poziomu oszacowanego ryzyka (kolumny tablicy), lokalizacji strefy obserwacji i rodzaju aktywności, które mają być poddane obserwacji. W niektórych przypadkach (w przypadku stref

ogrodzenia i łączników komunikacyjnych), po wprowadzeniu mechanizmu detekcji ruchu w danej strefie, dopuszcza się zmniejszenie częstotliwości zapisu (fps), co zaznaczono „*” w ostatniej kolumnie tablicy.

Tab. 1. Zalecane parametry systemu VSS – zależność parametrów jakościowych obrazu od lokalizacji strefy obserwacji, aktywności, i oszacowanego poziomu ryzyka [4].

Lokalizacja strefy	Rodzaj aktywności	Cel obserwacji i jakość obrazu w zależności od poziomu ryzyka		
		Ryzyko wysokie	Ryzyko średnie	Ryzyko niskie
Parking samochodowy – dostęp pojazdów	Rejestracja numerów	Rejestracja numerów 12,5fps	Rejestracja numerów 12,5fps	Rejestracja numerów 12,5fps
Parking samochodowy – parkowanie	Kradzieże, napady	Obserwacja + PTZ 6fps	Detekcja + PTZ 6fps	Obserwacja 6fps
Parking samochodowy – dostęp pieszych	Kradzieże, napady	Rozpoznanie 6fps	Obserwacja 6fps	Obserwacja 2fps
Stojak na rowery	Kradzież, wandalizm	Rozpoznanie 6fps	Obserwacja 6fps	Obserwacja 6fps
Ogrodzenie	Ruch	Detekcja 2fps	Detekcja 2fps	Detekcja 6fps *
Front budynku	Jakakolwiek	Obserwacja + PTZ 12,5fps	Detekcja + PTZ 6fps	Obserwacja 2fps
Powierzchnia handlowa/ulica	Jakakolwiek	Obserwacja + PTZ 12,5fps	Obserwacja + PTZ 6fps	Obserwacja 2fps
Łączniki (schody ruchome, windy, schody)	Jakakolwiek	Obserwacja 6fps	Obserwacja 6fps	Obserwacja 6fps *
Obszar baru	Zachowania antyspołeczne, kradzież, napad	Obserwacja 12,5fps	Obserwacja 6fps	Obserwacja 6fps
Liczenie gotówki	Kradzieże, oszustwo	Identyfikacja 12,5fps	Identyfikacja 6fps	Identyfikacja 6fps
Podjazd, zatoka, rampa	Kradzież, wandalizm, zdrowie, bezpieczeństwo	Obserwacja 6fps	Obserwacja 6fps	Obserwacja 2fps

3. KLASYFIKACJA STOPNI ZABEZPIECZENIA W ELEKTRONICZNYCH SYSTEMACH KONTROLI DOSTĘPU

W dwóch nowych normach IEC dotyczących elektronicznych systemów kontroli dostępu (EACS) [3], [4] wykorzystano przedstawione wyżej zasady klasyfikacji – oparte na oszacowaniu ryzyka w strefie kontrolowanej przez dane przejście.

Stopnie zabezpieczenia powinny być określone indywidualnie dla wejścia i wyjścia, dla każdego punktu kontroli dostępu. **W tym samym systemie mogą być wykorzystywane punkty o różnych stopniach zabezpieczenia. Natomiast stopień zabezpieczenia punktów**

„na tej samej drodze” – wspólnych dla danej strefy, powinien być taki jak najwyższy stopień zabezpieczenia punktu tej strefy, zlokalizowanego np. na końcu strefy.

W tablicy 2 przedstawiono ogólną zasadę określania stopni zabezpieczenia punktów kontroli dostępu. W przypadkach punktów EACS stopni 2, 3 i 4, gdzie celem kontroli dostępu jest **odstraszenie, opóźnienie, wykrycie i pomoc w identyfikacji atakujących** – osób nieuprawnionych do dostępu, zasoby mają wartość średnią do bardzo wysokiej, a atakujący po nieudanej próbie mogą porzucić zamiar uzyskania dostępu, gdy się zorientują, że mogą być zidentyfikowani (i ujęci w przypadku systemów EACS stopnia 3 i 4).

Tab. 2. Stopnie zabezpieczenia w elektronicznych systemach kontroli dostępu [3]

Stopień zabezpieczenia	1	2	3	4
Poziom ryzyka	Ryzyko niskie	Ryzyko niskie do średniego	Ryzyko średnie do wysokiego	Ryzyko wysokie
Zastosowanie	aspekty organizacyjne, zabezpieczanie zasobów niskiej wartości	aspekty organizacyjne, zabezpieczanie zasobów niskiej do średniej wartości	mniej aspekty organizacyjne, zabezpieczanie zasobów handlowych od średniej do wysokiej wartości	głównie zabezpieczanie bardzo wysokich wartości handlowych albo infrastruktury krytycznej
Doświadczenie/ wiedza adwersarzy/atakujących	małe doświadczenie, mała wiedza o EACS, brak wiedzy o tokenach i technikach IT małe środki finansowe na dokonanie ataków	średnie doświadczenie i wiedza o EACS, mała wiedza o tokenach i technikach IT małe do średnich środki finansowe na dokonanie ataków	szerokie doświadczenie i wiedza o EACS, średnia wiedza o tokenach i technikach IT średnie środki finansowe na dokonanie ataków	bardzo szerokie doświadczenie i wiedza o EACS, szeroka wiedza o tokenach i technikach IT duże środki finansowe na dokonanie ataków
Typowe przykłady	hotel	biura, małe do średnich przedsiębiorstwa.	przemysł, administracja, finanse	obszary wysoce wrażliwe (obiekty wojskowe, rządowe, R&D, obszary produkcji krytycznej)

Niżej przedstawiono kilka zasad projektowania systemów EACS zalecanych w normie [4]. W procesie projektowania systemu EACS stopień zabezpieczenia powinien być określany dla każdego punktu oddzielnie biorąc pod uwagę potrzeby sterowania dotyczące wejścia i wyjścia. W tej samej instalacji mogą być stosowane przejścia kontrolowane o różnym stopniu zabezpieczenia. Gdy okazuje się niepraktycznym instalowanie w jednym systemie punktów o różnych stopniach zabezpieczenia, zezwala się na systemy oddzielne.

Stosowane uwierzytelnienie powinno być takie, jak te z punktu o najwyższym stopniu zabezpieczenia. Warianty sterowania dostępem powinny np. uwzględniać: **wejście/wyjście, kontrolę użyczenia (antypassback), blokowanie oraz zawsze w przypadku zagrożeń tj. pożar, zagrożenia od środowiska odblokowanie przejścia – obojętnie.**

W normie [3] podano po raz pierwszy bardzo obszerny wykaz terminów i definicji liczący 119 pozycji, wiele z nich nie było dotąd znanych i stosowanych w polski nazewnictwie. Przedstawiono również 28 wymagań związanych z autoochroną (antysabotażem) systemu. Przykładowo, niezależnie od stopnia zabezpieczenia EACS, ochrona szczelności obudowy urządzenia ACS umieszczonego na zewnątrz kontrolowanego obszaru powinna być w każdym przypadku IP4X i jej wytrzymałość na sabotaż/uderzenia IK04.

Norma stawia szczegółowe liczne wymagania dotyczący czytników – wskaźników sygnalizujących alarmy i stany przejścia, podano w niej 47 wymagań związane np. z: wizualizacją poleceń dla użytkownika, alarmami różnego

typu, utratą łączności, awarią zasilania. W wymaganiach dotyczących rozpoznania wskaźnik fałszywych akceptacji FAR_{eff} w czynnikach z biometrią powinien być max 0,3% (przejście 3 stopnia) i 0,1% (przejście 4 stopnia). W systemie 4 stopnia powinna być realizowana sygnalizacja przymusu, a monitorowanie łączności powinno następować odpowiednio co 10min i 2min. Czasy podtrzymania zasilania powinny wynosić przy systemach 3 i 4 stopnia odpowiednio 2h i 4h (jest to fundamentalne wymaganie postawione po raz pierwszy w normach dotyczących systemów kontroli dostępu).

Zasady stosowania EACS przedstawione w [4] obejmują szacowanie ryzyka (*risk assessment*) otwierające proces stosowania EACS, przeprowadza się je w pierwszym etapie „planowanie systemu”, dokonując oceny: zasobów, zagrożeń, ryzyka i tego „co należy zrobić”. W procesie oceny zasobów należy je zinventaryzować i ocenić ich cechy tj.: poufność, integralność i dostępność, wyróżniając zasoby ludzkie. Rozpatrując zagrożenia należy odpowiedzieć na pytania: przeciwko komu/czemu? kto? co? kiedy? gdzie? dlaczego? jak?

Szacując ryzyko zwraca się uwagę na możliwość wykorzystania przez intruzów słabości danego obiektu – kontrolowanego obszaru. W ostatnim etapie planowania stawia się przedstawione wyżej wymagania i ocenia skuteczność kontroli dostępu i koszt jej realizacji. Postępując w sposób jaki zaleca norma wykrywa się i redukuje słabości chronionego obiektu przez ograniczenie skutków nieuprawnionego dostępu. Proces szacowania ryzyka kończy się określeniem stopnia zabezpieczenia każdego punktu EACS.

3. PODSUMOWANIE

Ogólna analiza postanowień nowych norm dotyczących systemów alarmowych VSS i EACS wykazuje, że fundamentalnym etapem procesu budowy tych systemów jest analiza – szacowanie ryzyka prowadzona szczegółowo dla **każdej strefy obserwacji wizyjnej i każdego punktu kontroli dostępu**. Oszacowanie ryzyka prowadzi następnie do wyznaczenia stopnia zabezpieczenia (*security grade*) pozwalając na dobór urządzeń alarmowych spełniających szczegółowe wymagania norm przedmiotowych – urządzeń „dostosowanych – dopasowanych” w trakcie realizacji tego procesu do oszacowanego ryzyka. Szczegółowe wymagania mogą dotyczyć np. zabezpieczenia przed sabotażem i poziomów dostępu do systemów przez użytkowników.

Ogólna metodyka szacowania ryzyka jest szczegółowo przedstawiona w innych normach [6] i [7] można również korzystać w tym przypadku z wymagań stawianych zarządzaniu bezpieczeństwem informacji [8], szczególnie z [9]. Wydaje się, że powinna być opracowana osobna „wspólna” norma albo specyfikacja techniczna „Systemy alarmowe – Zarządzanie ryzykiem – Zasady i wytyczne” dotycząca zarządzania ryzykiem w elektronicznych systemach alarmowych, scalająca przedstawione wyżej problemy dotyczące wyznaczania stopnia zabezpieczenia tych systemów, ułatwiając szczególnie planowanie i projektowanie złożonych i rozległych systemów alarmowych 3 i 4 stopnia zabezpieczenia. W 2016r POLALARM zamierza przeprowadzić konferencję, w zakresie omówionych wyżej problemów przeznaczoną szczególnie dla dystrybutorów, rzeczoznawców oraz osób planujących rozwiązania VSS i EACS.

BIBLIOGRAFIA

1. PN-EN 50132-1:2010 Systemy alarmowe - Systemy dozoru CCTV stosowane w zabezpieczeniach – Część 1: Wymagania systemowe
2. IEC 62676-4:2014 Video surveillance systems in security applications – Part 4: Application guidelines
3. IEC 60839-11-1:2013 Alarm and electronic security systems – Part 11-1: Electronic access control systems – System and components requirements
4. IEC 60839-11-2:2014 Alarm and electronic security systems – Part 11-2: Electronic access control systems – Application guidelines
5. PN-EN 50131-1:2009 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 1: Wymagania systemowe
6. PN-ISO 31000:2012 Zarządzanie ryzykiem – Zasady i wytyczne
7. IEC/ISO 31010:2009 Risk management – Risk assessment techniques
8. PN-ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania
9. PN-ISO/IEC 27005:2010 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.

- dr inż. Andrzej Ryczer, Stowarzyszenie „POLALARM”
Polski Komitet Normalizacyjny, Komitet Techniczny KT 52
Treść pierwotna opublikowana
w Systemach Alarmowych Nr 1/2014

Przegląd prasy branżowej

Witam Czytelników,

Już tradycyjnie zacznę przegląd prasy branżowej od lektury Przeglądu Technicznego. Z biegiem czasu moje zainteresowanie tym pismem wzrasta, dlatego od niego zaczynam. Powody są dwa. Po pierwsze, jest ono prowadzone na bardzo wysokim poziomie redakcyjnym, czego życzę i innym wydawnictwom, po drugie Przegląd Techniczny zamieszcza sporo artykułów o tematyce, która może zainteresować każdego z nas.

I tak, na stronie 15 numeru 21-22 2015 Przeglądu Technicznego zamieszczony jest artykuł pod tytułem „Pożerać CO₂”. Jak dotąd wszystkie media głoszą apokaliptyczną wizję o efekcie cieplarnianym powodowanym nadmierną emisją dwutlenku węgla do atmosfery. Tymczasem okazuje się, że podczas produkcji biopaliw trzeciej generacji z wykorzystaniem sztucznie hodowanych alg, dwutlenek węgla jest podstawowym produktem przetwarzanym przez te rośliny. Biolodzy twierdzą, że podczas produkcji biopaliw czwartej generacji będzie można wykorzystać dwutlenek węgla i inne odpady wytwarzane przez konwencjonalne elektrownie. Wizja ciekawa, lecz okazuje się że jest trudna w realizacji, gdyż protestują przeciwko temu rolnicy. Hodowla alg na masową skalę spowodowałaby ograniczenie powierzchni gruntów przeznaczonych na produkcję żywności. Głównym oponentem jest Unia Europejska. I jak tu nie być eurosceptykiem? Może niedługo, nie oglądając się na zakazy, w gospodarstwach przydomowych, albo nawet w doniczkach na balkonie sami zaczniemy produkować paliwo dla naszych samochodów?

Innym, ciekawym materiałem, zamieszczonym na stronie 24 tego samego numeru Przeglądu Technicznego jest artykuł „Aby las był bezpieczny”. Chodzi o tereny leśne, na których kiedyś, bez jakichkolwiek uzgodnień z prawowitymi właścicielami utworzone zostały ogromne poligony wojskowe. Przykładem może być Borne Sulimowo, a także inne tereny opuszczone przez jednostki wojskowe. Na tych terenach znajdują się olbrzymie ilości niebezpiecznych materiałów, pozostawionych jeszcze przez Armię Czerwoną i Ludowe Wojsko Polskie. Okazuje się, że przywrócenie tych terenów do normalnej eksploatacji wiąże się z ogromnymi kosztami, gdyż kilkadziesiąt lat temu nikt nie zadał sobie najmniejszego trudu by sporządzić choćby szkieletową dokumentację miejsc składowania odpadów chemicznych czy złomowisk niewybuchów artyleryjskich. No cóż, jaki pokój, takie meble, na szczęście tą epokę mamy już za sobą, a niebezpieczne lasy pozostały.

W numerze 23-24 2015 Przeglądu Technicznego znalazłem artykuł, który mnie zdecydowanie zaniepokoił. Chodzi o IoT, czyli Internet Rzeczy. Jeszcze niedawno sam się dziwiłem, słysząc opowieści o pralkach podłączonych do Internetu. Teraz zmieniłem zdanie, zmusiły mnie do tego obiektywne fakty. Internet Rzeczy jest szybko rozwijającym się rynkiem, który może stanowić podstawę biznesu dla wielu firm specjalizujących się w teleinformatyce. Nikomu już nie imponują nowoczesne domy, w których możemy włączyć ogrzewanie na dwa dni przed przyjazdem na zimowe wakacje. Na podobnej zasadzie nikogo nie ekscytują kamery, które pozwalają na odległość stwierdzić, czy dzieci i żona grzecznie się bawią gdy mąż jest w delegacji. To już było i wszystkim wydaje się oczywiste. Ale łazienkowa waga, która ma stałe połączenie z siecią przez interfejs Wi-Fi i regularnie wysyła wyniki naszych wagań do aplikacji działającej w chmurze, która oblicza wskaźnik masy ciała

i w formie wykresu oraz zaleceń co do bieżącej diety wysyła go na nasz smartfon, to zupełnie co innego. Marzyłaby się lodówka, która sprawdza co ma na półkach a czego zaczyna brakować, która składałaby elektroniczne zlecenie do e-sklepu gdy kończy nam się masło.

Podobną sytuację przewidział Stanisław Lem w swojej proroczej „Tragedii Pralniczej” napisanej jeszcze w 1957 roku, kiedy w Polsce szczytem technologii był radioodbiornik Pionier B2 (lampowy odbiornik baterijny, dla mieszkańców niezelektryfikowanych wsi). We wspomnianym opowiadaniu Stanisława Lema producenci pralek w pogoni za klientami wypuszczali na rynek coraz bardziej wyrafinowane modele. Z biegiem czasu pojawiły się pralki w kształcie kobiet, które poza praniem chusteczek do nosa nie robiły nic więcej, a wyspecjalizowały się w innych usługach i po jakimś czasie społecznym problemem stała się prostytucja wśród pralek. Czy do tego doprowadzi nas Internet Rzeczy? Zobaczmy, tymczasem zachęcam do lektury, zarówno Przeglądu Technicznego, jak i książek Stanisława Lema.

Wróćmy jednak do poważniejszych tematów i do lektury Systemów Alarmowych numer 6 / 2015. Tu tradycyjnie mamy do czynienia z podobnym co zawsze układem stron, z których kilkanaście jest poświęconych na krótkie informacje techniczne. Zawsze chwaliłem tą formę przekazu informacji, gdyż dzięki tym „news” można się szybko dowiedzieć o najnowszych trendach, technologiach etc. W części merytorycznej ten numer Systemów Alarmowych jest poświęcony serwerowniom, ich konstrukcji i ochronie, a także odprowadzaniu ciepła. Ciekawym problemem jest gaszenie pożarów w serwerowniach, bez uszkodzania zainstalowanych tam urządzeń. Tej tematyce poświęconych jest pierwszych 20 stron Systemów Alarmowych.

Na pozostałych stronach dominuje technika telewizyjna. I tak, na stronie 36 znajdziecie Państwo artykuł na temat systemów AHD, czyli analogowych systemów telewizyjnych o wysokiej rozdzielczości. Tytuł brzmi: „Mamy rewolucję!”. Ta rewolucja trwa już kilkanaście lat i niczego jeszcze nie zrewolucjonizowała. Pierwszą jaskółką, próbującą czynić wiosnę były systemy HD-SDI, po których obecnie nawet ślad nie został. Była to próba wykorzystania popularnego interfejsu SDI stosowanego w sprzęcie studyjnym, gdzie takie rozwiązanie miało rację bytu. Tymczasem w wizyjnych systemach dozorowych propozycja transmisji strumieni danych o przepływności rzędu 1,5GB/s okazała się pomyłką. W późniejszym okresie pojawiły się kolejne modyfikacje tych systemów. Obecnie mamy trzy dominujące, konkurujące ze sobą koncepcje, które poza szczegółami technologicznymi niczym się od siebie nie różnią. Mottem przewodnim jest hasło: „Zapomnij o TCP/IP, nie musisz się tego uczyć”, czyli odwołanie do najgorszych cech ludzkich, jakimi są lenistwo i nieuctwo. Na drugim miejscu wymieniana jest możliwość wykorzystania starych kabli koncentrycznych, pozostałych po zdemontowanych instalacjach CCTV. To jest czysta iluzja, gdyż stare kable z biegiem czasu straciły swoje parametry elektryczne i mechaniczne, popękały, nasiąkły wilgocią i nadają się jedynie do wymiany. Systemy AHD mają z reguły topologię gwiazdy, gdzie jednostka centralna jest sercem systemu. Awaria lub sabotaż tej jednostki powoduje, że cały system przestaje działać a wszystkie zgromadzone dane są bezpowrotnie tracone. Sygnały wizyjne z kamer są kodowane w tak egzotyczny sposób, że analogowe systemy HD różnych producentów nie są wzajemnie kompatybilne. Tą sytuację próbuje przełamać firma Dahua, która stworzyła własny standard i powołała stowarzyszenie mające zrzeszać producentów sprzętu zgodnego z tym standardem, dlaczego jednak na stronach 42 i 43 Systemów Alarmowych znajdujemy arty-

kuły na temat sieciowych urządzeń Dahua?

Rzeczywiście, na temat analogowych systemów HD gdybym chciałbym przestrzec wszystkich czytelników przed magią tego rozwiązania, tak jak przestrzegam przed kupowaniem perpetuum mobile do napędu samochodu, czy małej elektrowni termojądrowej z zimną fuzją do oświetlania domu.

Na stronie 50 Systemów Alarmowych znajdziecie państwo interesujący artykuł na temat wykorzystania dronów w różnych dziedzinach techniki, w tym także w systemach zabezpieczających. Te niewielkie i relatywnie tanie maszyny latające zyskują ostatnio na popularności, co spowodowało, że konieczne jest opracowanie nowych przepisów regulujących ich wykorzystanie. W ogólnie pojętych systemach alarmowych drony mogą być wkrótce wykorzystane jako narzędzie zwiadu dla załóg interwencyjnych. Po co wysłać dwie uzbrojone osoby do posesji, z której pochodzi alarm, jeśli można wysłać drona, który nie czeka w korkach ulicznych, więc dotrze na miejsce bardzo szybko i dostarczy materiału pozwalającego załodze na podjęcie optymalnej decyzji.

Tyle na temat Systemów Alarmowych. Na koniec przejdźmy do lektury Zabezpieczeń numer 5 (105)/2015. Tu już z okładki atakuje nas kolorowa reklama produktów włoskiej firmy Videotec. Znam tę firmę i jej wyroby bardzo dobrze, gdyż swego czasu produkowałem kamery o ekstremalnych parametrach, przeznaczone do obserwacji imprez masowych na stadionach, i w tych konstrukcjach wykorzystywałem obudowy i mechanizmy napędowe firmy Videotec. To co piszę, ma być nawiązaniem do poprzedniego komentarza na temat analogowych systemów HD.

Tak się składa, że znam osobiście konstruktorów z firmy Videotec, wielokrotnie z nimi rozmawiałem i wymienialiśmy poglądy na temat kierunków rozwoju telewizji dozorowej. Była to epoka, w której na rynku dominowały kamery CC-TV, czyli urządzenia analogowe, zgodne ze standardem PAL lub NTSC. Już wtedy próbowałem zachęcić kolegów z firmy Videotec by zainteresowali się sprzętem sieciowym, jednak wykazywali w tym względzie wyjątkowy opór. Twierdzili że to się nigdy nie upowszechni, bo jest zbyt drogie, zbyt skomplikowane i wymaga zbyt dużej wiedzy od instalatorów. Produkowali wtedy znakomite sterowniki automatyzujące pracę rozległych systemów CCTV, dostępne pod nazwą handlową „Albert”. Ich Alberty były do pracowane technologicznie i miały bardzo ciekawe funkcje, niedostępne w rozwiązaniach konkurencyjnych. I co z tego zostało? Po Albertach nie ma ani śladu, za to na okładce Zabezpieczeń widzimy sieciowe kamery Ulisse Radical firmy Videotec.

Artykuł mojego autorstwa, w którym próbuję omawiać te i inne perspektywy rozwoju wizyjnych systemów dozorowych znajdziecie Państwo na stronie 22 zabezpieczeń. Nie będę go omawiał, zapraszam do lektury, a wnioski wynikające z tego tekstu potwierdzają się na kolejnych stronach pisma.

Firma Bosch, która przez długie lata produkowała jedne z najlepszych na rynku kamer analogowych wpadła w podobną pułapkę jak Videotec i zaślepiona sukcesem rynkowym nie w porę zauważyła zmiany zmierzające do upowszechnienia systemów IP. W okresie przejściowym produkowane były kamery z adapterami sieciowymi, ale ciągle były to urządzenia analogowe o rozdzielczości SD. Obecnie, w ofercie firmy Bosch znajdują się prawie wyłącznie kamery sieciowe o bardzo wysokich parametrach, o czym możecie się Państwo przekonać czytając artykuł zamieszczony na stronie 30 zabezpieczeń. Traktuje on o kamerach panoramicznych, gdzie wymagana jest

bardzo wysoka rozdzielczość przetworników i obiektywów, zaś końcowy efekt jest silnie zależny od skuteczności i szybkości pracy procesorów DSP. Czy takie kamery mogłyby powstać w technologii analogowej? Odpowiedzcie sobie Państwo na to pytanie czytając wspomniany artykuł.

Kolejną zmianą, na którą chciałbym zwrócić Państwa uwagę jest pojawienie się nowego gracza na rynku wizyjnych systemów dozorowych. Jest to firma Canon, mająca ogromne doświadczenie i znakomite sukcesy na rynku kamer profesjonalnych i aparatów fotograficznych. Nie od rzeczy będzie wspomnieć o dużym doświadczeniu firmy Canon w produkcji bardzo dobrych obiektywów. Obecnie firma Canon próbuje zdobywać rynek systemów dozorowych, co jej się niechybnie uda, ze względu na ogromny potencjał intelektualny i technologiczny. Na razie są to jedynie skromne początki, ale wróżę tej firmie sukcesy na polskim rynku. Artykuł na temat produktów firmy Canon i jej planów rynkowych znajdziecie Państwo na stronie 26 Zabezpieczeń numer 5 (105) / 2015.

W końcowej części tego numeru znajdziecie państwo kilka artykułów na temat systemów sygnalizacji pożaru i ich integracji z innymi instalacjami zabezpieczającymi, a na ostatnich stronach zamieszczone są jak zwykle karty katalogowe produktów.

Na tym kończę zimowy przegląd prasy branżowej i życzę wszystkim sympatykom naszego biuletynu Wesołych Świąt.

Pozdrawiam wszystkich czytelników

- Andrzej Walczyk



W dniach 25-28 kwietnia 2016 roku w Poznaniu odbędzie się 21 edycja targów SECUREX, największych i najbardziej prestiżowych targów branży zabezpieczeń w Polsce oraz Europie Środkowo-Wschodniej. Targi te są areną prezentacji nowości rynkowych, ale jednocześnie to miejsce premier rozwiązań przyszłościowych.

Marka targów SECUREX gwarantuje, że każda ich edycja inspirowała rynek. Podczas targów w 2016 roku m.in. kontynuowana będzie prezentacja urządzeń i systemów alarmowych do ochrony przed włamaniem, napadem, kradzieżą (SSWiN), analogowego monitoringu wizyjnego (CCTV), ale także rozwiązań telewizji IP czy elektronicznych systemów zarządzania obiektami - inteligentnego budynku (BMS). Rozbudowany zostanie zakres ekspozycji urządzeń i systemów alarmowych oraz zabezpieczeń PPOŻ. Zdecydowanie obszernie zaistnieje temat bezpieczeństwa IT. Joanna Jasińska, wieloletni dyrektor targów SECUREX podkreśla, że problem zabezpieczeń dotyczy wszystkich, dlatego to właściwe miejsce dla firm, które chcą zaprezentować swoje produkty, urządzenia i systemy zabezpieczeń, ponieważ właśnie tutaj znajdą szerokie grono odbiorców.

- Na przestrzeni ostatnich lat branża zabezpieczeń rozwija się w galopującym tempie. Musi się ona dopasować do potrzeb rynku, który nieustannie rozwija się i modernizuje m.in. w zakresie bezpieczeństwa IT, ppoż, systemów alarmowych oraz inteligentnych rozwiązań dla budynków. Temat zabezpieczeń dotyczy każdej gałęzi przemysłu i jest na co dzień obecny w życiu społeczeństwa. – podkreśla

Joanna Jasińska, dyrektor targów. - Targi Securex to miejsce prezentacji premierowych systemów i rozwiązań dla ogromnego grona odbiorców. Każda firma potrzebuje zabezpieczenia swojej działalności i informacji jakie systemy będą dla niej optymalne. Od rozwiązań mechanicznych, przez bezpieczeństwo informacji i wykwalifikowane służby, po te coraz bardziej zaawansowane, mobilne.

Securex, czyli wielkoformatowe bezpieczeństwo w jakości FullHD

SECUREX to wiodące wydarzenie biznesowe dla branży. Każdorazowo ekspozycja imponuje rozmiarem i różnorodnością prezentowanych produktów. Wachlarz firm oraz asortymentu jest bardzo szeroki. Od zabezpieczeń mechanicznych w postaci zamków, drzwi, bram po spektrum najnowszych osiągnięć z dziedziny telewizji dozorowej, przez prezentację centrali zarządzających bezpieczeństwem całych obiektów, w tym np. przeciwpożarowych systemów instalacyjnych, kompleksowych rozwiązań IT, zawierających m.in. wielofunkcyjne kontrole dostępu, aż po centra monitorowania alarmów. To tutaj swoją ofertę prezentują liderzy rynku zabezpieczeń, ale również przedsiębiorstwa, których logo nie jest rozpoznawalne na rynku międzynarodowym, a w swojej ofercie posiadają innowacyjne rozwiązania dla zabezpieczeń budynków lub posiadające np. oprogramowania i systemy użyteczne w procesach zabezpieczania działalności konkretnej branży. Wynika to z faktu, że od lat organizator targów dostarcza wystawcom zwiedzających, którzy często stają się dla firm klientem nie jednorazowym lecz powtarzalnym.

Poza profesjonalną ekspozycją argumentami, które przyciągają zwiedzających są wydarzenia merytoryczne oraz współpraca organizatora z najważniejszymi w kraju organizacjami i stowarzyszeniami działającymi na polu bezpieczeństwa takimi jak: ministerstwa, Komenda Główna Policji, GIODO, a patronat branżowy nad targami obejmują Polska Izba Systemów Alarmowych, POLALARM Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem czy Polska Izba Ochrony. Dzięki poparciu administracji państwowej oraz partnerów branżowych targi SECUREX są źródłem fachowej wiedzy, miejscem szkoleń i merytorycznych konferencji, a także wydarzeń specjalnych takich jak: V Mistrzostwa Polski Instalatorów.

Aby zabezpieczyć sobie najlepsze ceny i miejsce

warto zgłosić się jeszcze w tym roku. Duże zainteresowanie wystawców targami SECUREX zapowiada, że będzie to wydarzenie znaczącej wagi, w którym udział z pewnością wzmocni zarówno promocję produktów jak i wizerunek firmy. Już dziś wiadomo, którzy liderzy zgłosili swoje uczestnictwo. Na targi SECUREX zapraszają m.in. AAT HOLDING, ALPOL, AMBIENT SYSTEM, AXIS COMMUNICATIONS POLAND, BOSCH, C&C PARTNERS, CANON POLSKA, DAHUA VISION TECHNOLOGY, ELA COMPIL, GUNNEBO POLSKA, HIKVISION POLAND, JANEX INTERNATIONAL, POLON ALFA, PROFICCTV, SATEL, UTC FIRE&SECURITY POLSKA, XTRALIS UK.

Międzynarodowe Targi Poznańskie podkreślają, że doskonałe kontakty, wypracowane przez lata ze środowiskiem fachowców, pozwalają za każdym razem na tworzenie wartościowego merytorycznie i biznesowo wydarzenia, które zawsze prezentuje najwyższą jakość. Takich targów po prostu nie można przegapić, a swój sukces trzeba zabezpieczyć. Im wcześniej tym lepiej.

- MTP

Nowe prawo dla stowarzyszeń

26 października 2015 r. prezydent Andrzej Duda podpisał ustawę o zmianie ustawy - Prawo o stowarzyszeniach oraz niektórych innych ustaw. To pierwsza tak znacząca zmiana w ustawie uchwalonej ćwierć wieku temu. Czy nowelizacja będzie impulsem do rozwoju trzeciego sektora? Co konkretnie się zmieni?

Potrzeba zmian w ustawie od dawna była postulowana przez środowisko organizacji pozarządowych. Jakie zmiany wprowadza nowelizacja?

7 osób zamiast 15

W obecnym stanie prawnym do zarejestrowania stowarzyszenia potrzeba jest inicjatywa aż 15. obywateli. Nowelizacja zmniejsza wymaganą liczbę założycieli do siedmiu. To chyba najbardziej symboliczna z wprowadzanych zmian. Wiąże się z nią duże nadzieje. Nasze przepisy upodobnią się w tym zakresie do przepisów innych krajów europejskich. Liczba 15 jest barierą w wielu środowiskach lokalnych. Likwidacja tej bariery ma spowodować ożywienie się postaw obywatelskich – liczba stowarzyszeń wzrośnie. O tym, jak bardzo, będziemy mogli się przekonać już w drugiej połowie 2016 r.

Szybsza rejestracja

Do tej pory sądy miały trzy miesiące na rozpoznanie wniosku o rejestrację stowarzyszenia. Teraz będzie szybciej - stowarzyszeń dotyczyć będą ogólne terminy zapisane w ustawie o Krajowym Rejestrze Sądowym, które na załatwienie spraw dają tydzień.

Mniej nadzoru starosty

– To dobra zmiana – ocenia Renata Niecikowska ze Stowarzyszenia Klon/Jawor. – Oznacza mniej biurokracji, tam, gdzie jest ona zbyt duża i blokuje rejestrację lub ją bardzo wydłuża, a zdarza się, że wynika z nadinterpretacji prawa przez starostwa. Kontrola KRS w tym zakresie w zupełności wystarczy.

Nowe stowarzyszenia zwykłe

W Polsce mamy dwa rodzaje stowarzyszeń: rejestrowe i zwykłe. Stowarzyszeń zwykłych jest dużo mniej niż rejestrowych, do tej pory nie miały one osobowości prawnej, mogły być finansowane jedynie ze składek. Nowelizacja to zmienia: nadaje im tzw. ułomną osobowość prawną. Nowe zwykłe będą miały prawo do korzystania z dotacji (czyli np. do udziału w konkursach ogłaszanych przez samorząd gminy). Finansowanie działalności będzie też możliwe ze środków z darowizn, spadków, zapisów, dochodów z majątku stowarzyszenia oraz ofiarności publicznej. Stowarzyszenie zwykłe będzie mogło ubiegać się o status organizacji pożytku publicznego i zbierać 1 procent. Zwykłe znacznie bardziej zaczną przypominać rejestrowe – zbliżą się do nich, jeśli chodzi o możliwości formalne. Czego nie będą mogły robić? Nie będą prowadzić działalności gospodarczej oraz odpłatnej działalności pożytku. Nie będą też tworzyć jednostek terenowych. Nadal wystarczą trzy osoby do założenia takiego stowarzyszenia.

- W mojej ocenie to właśnie stowarzyszenia zwykłe najczęściej zyskają - mówi Rafał Kowalski z portalu organizacji pozarządowych ngo.pl. – Dzięki nowelizacji uzyskały ułomną osobowość prawną. Do tej pory stowarzyszenie zwykłe były na marginesie, mogły bardzo niewiele. Teraz będzie to prosta forma aktywności społecznej, ale dająca realne możliwości działania np. startowania w konkursach i korzystania z dotacji - podkreśla.

Zarząd może zarabiać

Jednym z celów nowelizacji było rozwiązanie wątpliwości co do możliwości wynagradzania osób pracujących w stowarzyszeniach, również tych, które są członkami organizacji i zasiadają w ich władzach. Nowelizacja wskazuje więc wyraźnie, że możliwe jest wynagradzanie członków zarządu "za czynności związane z pełnioną funkcją". Nie chodzi tu o wynagradzanie samego faktu bycia członkiem zarządu, ale o opłacanie konkretnej, często wymagającej dużych kompetencji i zaangażowania pracy, świadczonej na rzecz stowarzyszenia.

Większość zapisów ustawy o zmianie ustawy - Prawo o stowarzyszeniach wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia, czyli w drugim kwartale 2016 roku.

- Portal.ngo.pl

Usługi ochrony osób i mienia - koncesje

INFORMACJA dotycząca ubiegania się, rozszerzenia lub zmiany koncesji w zakresie regulowanym ustawą z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2005 r. Nr 145, poz. 1221, z późn. zm.).

Wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia wymaga uzyskania koncesji Ministra Spraw Wewnętrznych, określającej zakres i formę jej prowadzenia.

(art. 15 ust. 1 ustawy o ochronie osób i mienia)

Ochrona osób i mienia realizowana jest w formie bezpośredniej ochrony fizycznej lub zabezpieczenia technicznego.

(art. 3 ustawy o ochronie osób i mienia)

Postępowanie administracyjne o udzielenie koncesji trwa (stosownie do przepisów Kodeksu postępowania administracyjnego) – około 2 miesięcy od daty złożenia, poprawnie wypełnionego wniosku (wraz z wymaganymi załącznikami).

Do terminów załatwienia sprawy, przewidzianych w przepisach Kodeksu postępowania administracyjnego (Kpa) nie wlicza się terminów przewidzianych w przepisach prawa dla dokonania określonych czynności, okresów zawieszenia postępowania oraz okresów opóźnień spowodowanych z winy strony albo z przyczyn niezależnych od organu (art. 35 Kpa).

W przypadku zaistniałej przeszkody uniemożliwiającej usunięcie braków formalnych w terminie dłuższym niż 7 dni, strona może wystąpić o zawieszenie postępowania administracyjnego, co wstrzymuje bieg terminów przewidzianych w kodeksie.

Wniosek o zawieszenie postępowania, jak również o podjęcie zawieszonego postępowania nie podlega opłacie skarbowej.

(art. 98 § 1 oraz art. 103 Kpa)

Koncesję wydaje się na wniosek przedsiębiorcy będącego osobą fizyczną (wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej – CEIDG) lub przedsiębiorcy będącego osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonującą we własnym imieniu działalność gospodarczą, zarejestrowanemu w rejestrze przedsiębiorców Krajowego Rejestru Sądowego (KRS).

Uwaga!

Należy pamiętać, iż przedsiębiorca ubiegający się o Koncesję powinien wskazać w przedmiocie działalności Polskiej Klasyfikacji Działalności (PKD) następujące podklasy:

80.10.Z i 80.20.Z – dotyczy usług ochrony osób i mienia realizowanych w formie bezpośredniej ochrony fizycznej;

80.20.Z – dotyczy usług ochrony osób i mienia realizowanych w formie zabezpieczenia technicznego.

Wniosek o udzielenie lub zmianę koncesji określa wzór formularza, który został wprowadzony rozporządzeniem Ministra Spraw Wewnętrznych z dnia 6 grudnia 2013 r. w sprawie wzoru wniosku o udzielenie lub zmianę koncesji na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia (Dz. U. poz. 1566) – vide załącznik nr 1 do informatora.

Koncesję wydaje się na wniosek przedsiębiorcy będącego:

1. osobą fizyczną, jeżeli jest on wpisany na listę kwalifikowanych pracowników ochrony fizycznej lub kwalifikowanych pracowników zabezpieczenia technicznego;
2. osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonującą we własnym imieniu działalność gospodarczą, jeżeli na listę kwalifikowanych pracowników ochrony fizycznej lub kwalifikowanych pracowników zabezpieczenia technicznego jest wpisana co najmniej jedna osoba będąca współnikiem spółki jawnej lub komandytowej, członkiem organu zarządzającego, prokurentem lub pełnomocnikiem ustanowionym przez przedsiębiorcę do kierowania działalnością określoną w koncesji, a pozostałe osoby uprawnione do reprezentacji przedsiębiorcy nie były karane za przestępstwo umyślne lub umyślne przestępstwo skarbowe.

Uwaga!

Obywatele państw członkowskich Unii Europejskiej (UE), państw członkowskich Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stron umowy o Europejskim Obszarze Gospodarczym (EOG) oraz obywatele państw niebędących stronami umowy o EOG, którzy mogą korzystać ze swobody przedsiębiorczości na podstawie umów zawartych przez te państwa ze Wspólnotą Europejską i jej państwami członkowskimi, podejmując działalność gospodarczą na terytorium RP, podlegają przepisom prawa polskiego i mają takie same prawa i obowiązki, jak przedsiębiorcy polscy.

Wniosek o udzielenie koncesji powinien zawierać:

3. firmę przedsiębiorcy (zgodną z wpisem do CEIDG lub KRS), oznaczenie jego siedziby i adresu lub adresu zamieszkania - (w przypadku przedsiębiorcy będącego osobą fizyczną za adres jego siedziby uznaje się adres jego zamieszkania);
4. numer w rejestrze przedsiębiorców w KRS albo informację o wpisie do CEIDG oraz numer identyfikacji podatkowej (NIP);
5. określenie zakresu i formy (form) wykonywanej działalności gospodarczej objętej koncesją;
6. datę rozpoczęcia wykonywania działalności gospodarczej objętej koncesją – (wpisana data rozpoczęcia wykonywania koncesjonowanej działalności gospodarczej nie może być datą wcześniejszą niż data wydania kon-

cesji – należy zatem pamiętać, że postępowanie o udzielenie koncesji trwa około 2 miesięcy (lub dłużej) - lub zaznaczyć „data doręczenia koncesji”);

7. adresy miejsc wykonywania działalności gospodarczej objętej wnioskiem, w tym przechowywania dokumentacji, o której mowa w art. 19 ust. 1 pkt 2 i 3 ustawy o ochronie osób i mienia;
 8. dane przedsiębiorcy będącego osobą fizyczną, osób uprawnionych lub wchodzących w skład organu uprawnionego do reprezentowania przedsiębiorcy, prokurentów oraz pełnomocnika ustanowionego w celu kierowania działalnością określoną w koncesji;
 9. informacje o posiadanych koncesjach, zezwoleniach lub wpisach do rejestru działalności regulowanej;
 10. oświadczenie o niezaleganiu z wpłatami należności budżetowych przedsiębiorcy będącego:
 - a. osobą fizyczną w brzmieniu: „Oświadczam, że nie zalegam z wpłatami należności budżetowych”;
 - b. osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonującą we własnym imieniu działalność gospodarczą proponuje się treść: „Oświadczam, że przedsiębiorca, tj. /firma przedsiębiorcy/ nie zalega z wpłatami należności budżetowych.”
- zawierające obligatoryjną klauzulę o następującej treści „Jestem świadomy(a) odpowiedzialności karnej za złożenie fałszywego oświadczenia” – klauzula ta zastępuje pouczenie organu o odpowiedzialności karnej za składanie fałszywych zeznań.
- (art. 17 ust. 3 pkt 8 i art. 17 ust. 4 ustawy o ochronie osób i mienia)

Uwaga!

Ww. oświadczenie przedsiębiorca składa w formie załącznika do wniosku tylko w przypadku nie złożenia oświadczenia na obowiązującym formularzu wniosku o udzielenie lub zmianę koncesji.

Do wniosku przedsiębiorca dołącza dokumenty w formie oryginału, poświadczonej kopii lub poświadczono-ego tłumaczenia.

Zamiast oryginału dokumentu strona może złożyć odpis dokumentu, jeżeli jego zgodność z oryginałem została poświadczona przez organ który go wydał, notariusza albo przez występującego w sprawie pełnomocnika strony będącego adwokatem lub radcą prawnym. (art. 76a § 1 i 2 Kpa)

WYKAZ NIEZBĘDNYCH DOKUMENTÓW W POSTĘPOWNIU O UDZIELENIE KONCESJI

Do wniosku o udzielenie koncesji należy dołączyć:

1. zaświadczenie o wpisie na listę kwalifikowanych pracowników ochrony fizycznej lub kwalifikowanych pracowników zabezpieczenia technicznego,
2. oświadczenie o niekaralności:
 - a. przedsiębiorcy będącego osobą fizyczną (zał. nr 2);
 - b. przedsiębiorcy, będącego osobą prawną lub jednostką organizacyjną niebędącą osobą prawną, której odrębna ustawa przyznaje zdolność prawną – wykonującą we własnym imieniu działalność gospodarczą (zał. nr 3);
- c. oświadczenia osób, o których mowa w art. 17 ust. 3

pkt 6 ustawy o ochronie osób i mienia (zał. nr 2) – (np.: wspólników spółki jawnej, członków zarządu oraz prokurentów i pełnomocników ustanowionych do kierowania działalnością określoną w koncesji), w tym oświadczenia o niekaralności obywateli państw członkowskich UE, państw członkowskich EFTA - stron umowy o EOG oraz obywateli państw niebędących stronami umowy o EOG, które mogą korzystać ze swobody przedsiębiorczości na podstawie umów zawartych przez te państwa ze Wspólnotą Europejską i jej państwami członkowskimi, zgodnie z art. 17 ust. 5 pkt 2 ustawy o ochronie osób i mienia;

3. poświadczone tłumaczenie zaświadczenia o niekaralności przedsiębiorcy oraz osób innych niż wymienione w pkt 2;
4. listę udziałowców lub akcjonariuszy, posiadających co najmniej 50 % udziałów lub akcji - w przypadku przedsiębiorcy innego niż osoba fizyczna;
5. oryginał dowodu opłaty skarbowej - za wydanie lub zmianę koncesji (patrz tabela);
6. oryginał pełnomocnictwa lub poświadczoną jego kopię - w przypadku ustanowienia pełnomocnika do reprezentowania przedsiębiorcy przed organem koncesyjnym wraz z dowodem wniesionej opłaty skarbowej (patrz tabela).

Uwaga!

W przypadku ustanowienia pełnomocnika do reprezentowania przedsiębiorcy przed organem koncesyjnym, korespondencja w sprawie będzie doręczana wyłącznie pełnomocnikowi. (art. 40 § 2 Kpa)

Wnioskodawca zarówno w przypadku ubiegania się o udzielenie koncesji, jak i wnoszący o zmianę danych w niej zawartych, ma obowiązek dołączenia do wniosku tylko tych dokumentów, o których mowa w art. 17 ustawy o ochronie osób i mienia. Tym samym zbędne jest dołączanie innych dokumentów, np.: aktu notarialnego, umowy najmu nieruchomości, wydruku z CEIDG, odpisu KRS, uchwały, zapytania o udzielenie informacji o osobie lub o podmiocie zbiorowym z Krajowego Rejestru Karnego.

OPLATA SKARBOWA

Na podstawie art. 6 ust. 1 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz. U. z 2012 r. poz. 1282) obowiązek zapłaty opłaty skarbowej powstaje z chwilą złożenia wniosku o wydanie koncesji, zmianę jej zakresu itd., zaświadczenia, złożenia pełnomocnictwa do sprawy lub dokonania innych czynności urzędowych podlegających opłacie skarbowej. Opłatę skarbową za dokonanie ww. czynności urzędowych należy wnieść na podany poniżej numer rachunku bankowego:

Uwaga!

Do wniosku należy dołączyć oryginał dowodu uiszczenia należnej opłaty skarbowej.

INFORMACJA O WYSOKOŚCI OPLAT SKARBOWYCH

1. Udzielenie koncesji lub jej rozszerzenie o kolejny rodzaj działalności - 616 zł
2. Decyzja dotycząca przedłużenia terminu ważności Koncesji. Decyzja dotycząca rozszerzenia koncesji o kolejną formę działalności - 50% stawki za koncesję
3. Inna decyzja do której mają zastosowanie przepisy Kpa* (np. zmiana reprezentacji przedsiębiorcy, zmiana adresu siedziby przedsiębiorcy) - 10 zł,

4. Promesa – 98 zł

5. Zaświadczenie – 17 zł

6. Duplikat – 24 zł

7. Pełnomocnictwo do reprezentowania przedsiębiorcy przed organem koncesyjnym – 17 zł

* dotyczy zmiany danych zawartych w koncesji, o których mowa w art. 18 ust. 1 pkt 1, 1a, 2 i 4 ustawy o ochronie osób i mienia.

W przypadku nieuiszczenia opłaty skarbowej w wyznaczonym terminie wniosek podlega zwrotowi. (art. 261 § 1 i 2 Kpa)

OBOWIĄZKI INFORMACYJNE PRZEDSIĘBIORCY WOBEC ORGANU KONCESYJNEGO

Przedsiębiorca wykonujący działalność gospodarczą w zakresie usług ochrony osób i mienia jest obowiązany:

1. powiadomić organ koncesyjny o podjęciu, zawieszeniu i trwałym zaprzestaniu wykonywania działalności gospodarczej; (art. 19 ust. 1 ustawy o ochronie osób i mienia)
2. zgłaszać organowi koncesyjnemu zmiany danych, w terminie 14 dni od dnia ich powstania, dotyczących:
 - a. firmy przedsiębiorcy, oznaczenia jego siedziby i adresu albo adresu zamieszkania;
 - b. numeru w rejestrze przedsiębiorców w KRS albo informacji o wpisie do CEIDG oraz numeru identyfikacji podatkowej (NIP);
 - c. imion i nazwisk wspólników lub członków zarządu, prokurentów oraz pełnomocników w razie ich ustanowienia, ze wskazaniem osób wpisanych na listę kwalifikowanych pracowników ochrony fizycznej lub kwalifikowanych pracowników zabezpieczenia technicznego;
 - d. adresu miejsca wykonywania działalności gospodarczej.

(art. 18 ust. 3 ustawy o ochronie osób i mienia)

Uwaga!

W przypadku zmiany danych wymienionych w punkcie 2 lit. a), b) i d) należy złożyć tylko wypełniony formularz wniosku oraz dowód wniesienia opłaty skarbowej.

Zmiana danych w punkcie 2 lit. c) wymaga złożenia - nie tylko wypełnionego formularza wniosku i dowodu opłaty skarbowej, lecz również załączenia oświadczenia o niekaralności nowo powołanych osób (zał. nr 2) oraz oryginałów, poświadczonych kopii lub poświadczonych tłumaczeń wymaganych dokumentów – vide art. 17 ustawy o ochronie osób i mienia.

Natomiast wniosek o rozszerzenie zakresu koncesji o dodatkową formę działalności oraz przedłużenie terminu jej ważności powinien być złożony na tych samych zasadach, jak przy udzieleniu koncesji wraz z dowodem wniesienia należnej opłaty skarbowej.

OBOWIĄZKOWE UBEZPIECZENIE ODPOWIEDZIALNOŚCI CYWILNEJ PRZEDSIĘBIORCY

Zgodnie z art. 21a ust. 1 ustawy o ochronie osób i mienia przedsiębiorca wykonujący działalność gospodarczą w zakresie usług ochrony osób i mienia jest obowiązany do spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z ochroną osób i mienia. Szczegółowy zakres ubezpieczenia, termin

powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną określa rozporządzenie Ministra Finansów z dnia 9 grudnia 2013 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej przedsiębiorcy wykonującego działalność gospodarczą w zakresie usług ochrony osób i mienia (Dz. U. poz. 1550).

Uwaga!

W przypadku gdy przedsiębiorca nie zawarł umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku z ochroną osób i mienia organ koncesyjny, działając na podstawie art. 22 ust. 2 pkt 3 ustawy o ochronie osób i mienia, cofa udzieloną przedsiębiorcy koncesję.

Wykaz wybranych rozporządzeń dotyczących wykonywania działalności gospodarczej w zakresie usług ochrony osób i mienia

1. Rozporządzenie Ministra Finansów z dnia 9 grudnia 2013 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej przedsiębiorcy wykonującego działalność gospodarczą w zakresie usług ochrony osób i mienia (Dz. U. poz. 1550).
2. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 6 grudnia 2013 r. w sprawie wzoru wniosku o udzielenie lub zmianę koncesji na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia (Dz. U. poz. 1566).
3. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 16 grudnia 2013 r. w sprawie wzoru wniosku o wpis na listę kwalifikowanych pracowników ochrony fizycznej, wzoru wniosku o wpis na listę kwalifikowanych pracowników zabezpieczenia technicznego oraz wzoru zaświadczenia o wpisie na te listy (Dz. U. poz. 1628).
4. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 11 grudnia 2013 r. w sprawie legitymacji pracowników ochrony (Dz. U. poz. 1630).
5. Rozporządzenie Ministra Spraw Wewnętrznych z dnia 16 grudnia 2013 r. w sprawie dokumentowania działalności gospodarczej w zakresie usług ochrony osób i mienia (Dz. U. poz. 1739).

DANE KONTAKTOWE

Adres do korespondencji:
MINISTERSTWO SPRAW WEWNĘTRZNYCH
DEPARTAMENT ZEZWOLEŃ I KONCESJI
02-591 Warszawa, ul. Stefana Batorego 5

Biuro podawcze Ministerstwa
- wejście od ul. Rakowieckiej 2a
czynne: poniedziałek - piątek 8⁰⁰ - 16⁰⁰

Załączniki do strony (<http://msw.gov.pl>)

- Załącznik nr 1 - Wzór wniosku o udzielenie lub zmianę koncesji na wykonywanie działalności gospodarczej w zakresie usług ochrony osób i mienia
- Załącznik nr 2 - Wzór oświadczenia o niekaralności (osoba fizyczna)
- Załącznik nr 3 - Wzór oświadczenia o niekaralności (osoba prawna i jednostka organizacyjna niebędąca osobą prawną, której odrębna ustawa przyznaje zdolność prawną - wykonująca we własnym imieniu działalność gospodarczą)

- Załącznik nr 4 - Wzór oświadczenia o niezaleganiu przez przedsiębiorcę z wpłatami należności budżetowych (osoba fizyczna)
- Załącznik nr 5 - Wzór oświadczenia o niezaleganiu przez przedsiębiorcę z wpłatami należności budżetowych (os. prawna i jednostka organizacyjna niebędąca os. prawną, której odrębna ustawa przyznaje zdolność prawną).

- Źródło: <http://msw.gov.pl>

XIII FORUM INŻYNIERSKIE INNOWACYJNA TECHNIKA W MEDYCYNIE

Tradycyjnie podczas Targów "Innowacje-Technologie-Maszyny" w Poznaniu, 9 czerwca br. odbyło się XIII Forum Inżynierskie. Tym razem Forum poświęcone było tematyce innowacji technicznych w medycynie

Organizatorami XIII Forum, obok FSNT-NOT i Międzynarodowych Targów Poznańskich, była Izba Gospodarcza Medycyna Polska i Instytut Mechaniki Precyzyjnej. Forum wsparli: Polska Agencja Rozwoju Przedsiębiorczości, Zakład Ubezpieczeń Społecznych oraz firma COMP S.A.

Obrady XIII Forum Inżynierskiego otworzyła prezes Naczelnej Organizacji Technicznej **Ewa Mańkiewicz-Cudny**, życzenia owocnych obrad przekazał prezes Międzynarodowych Targów Poznańskich **Przemysław Trawa**.

Następnie, bez zbędnej zwłoki, przystąpiono do sesji panelowych. Jako pierwszy wystąpił prof. Piotr Augustyniak z Międzywydziałowej Szkoły Inżynierii Biomedycznej Akademii Górniczo-Hutniczej. Polecamy rozmowę z profesorem, zamieszczonej we wkładce poświęconej XIII Forum w 12 numerze „Przeglądu Technicznego”.

Kolejny mówca, Ryszard Kowski, wiceprzewodniczący komisji ds. procedur i audytów klinicznych w radiologii, przedstawił nowoczesną diagnostykę obrazową, jej możliwości, ale też i wiążące się z tym zagrożenia.

Podczas sesji panelowych przedstawione zostały prezentacje pokazujące najnowocześniejsze rozwiązania i materiały dla medycyny oraz zaprezentowano przykłady łączenia wiedzy medycznej z zasadami techniki i praktyki inżynierskiej w celu rozwoju urządzeń, procedur medycznych i rozwiązywania problemów związanych ze zdrowiem.

W panelu pn. „E-medycyna - innowacyjne rozwiązania teleinformatyczne w obsłudze, monitorowaniu i leczeniu pacjentów”, Ryszard Olszanowski, prezes Izby Gospodarczej Medycyna Polska, zaprezentował obraz kształtującego się rynku usług telemedycznych. Na konkretnych przykładach funkcjonujących już firm, swoje dokonania przedstawił:

- Tomasz Dziobiak – prezes MedGo Sp. z o.o. z Warszawy
- Patrycja Wizińska wraz z Anną Skotny-Krakowian ze Spółki NESTMEDIC z Wrocławia.

Kajetan Wojsyk, z-ca dyrektora Centrum Systemów Informatycznych Ochrony Zdrowia pokazał jak wkrótce wyglądać będzie elektroniczna dokumentacja pacjenta: internetowe konto pacjenta, e-recepta, e-skierowanie, e-zwolnienie itp., a Przemysław Tadla, dyrektor ds. strategii firmy MEDICALgorithmics, pokazał jak podbija się amerykański rynek urządzeniem do monitorowania pracy serca przez telefon.

W II panelu pn. „Hity techniczne” w medycynie wystąpili:

- prof. Paweł Olko, dyrektor Centrum Cyklotronowego Bronowice, który zaprezentował nieinwazyjne leczenie nowotworów
- prof. Przemysław Łoś z Instytutu Chemii Przemysłowej informując o diagnozowaniu wtórnej próchnicy zębów oraz o nowatorskiej metodzie przesiewowych badań osteoporozy
- dr inż. Igor Buzalewicz z Katedry Inżynierii Biomedycznej Politechniki Wrocławskiej - nt. optyki biomedycznej
- prof. Ludwik Pokora - prezes Centrum Techniki Laserowej z prezentacją tabletki laserowej zamiast lekowej
- Precyzja a medycyna, to III panel którego gospodarzem był Instytut Mechaniki Precyzyjnej oraz współpracujące z Instytutem przedsiębiorstwa. Prof. Tomasz Babul, dyrektor IMP oraz dr inż. Anna Makuch z IMP przedstawili Instytut oraz jego ofertę dla branży medycznej. Następnie efekty współpracy z IMP oraz własne innowacje i sukcesy zaprezentowali:
 - Łukasz Wasyluk ze Spółki BALTON
 - Krzysztof Nazar ze Spółki ALEX—MED.
 - dr inż. Lechosław Ciupik – prezes LFC – firmy badawczo-rozwojowo-wdrożeniowej w zakresie implantów wszczepianych do leczenia schorzeń kręgosłupa.



Pełna sala, w której odbywały się obrady świadczyła o zainteresowaniu i trafionej tematyce XIII Forum Inżynierskiego.

Po obradach merytorycznych Forum, przedstawiciele Zarządu Towarzystwa im. Hipolita Cegielskiego z Poznania, wręczyli członkom Zarządu FSNT-NOT, wiceprezesa Stefanowi Góralczykowi i Józefowi Suchemu medale "Labor omnia vincit" za stałe i praktyczne wcielenie w życie gospodarcze i publiczne maksymy Stanisława Staszica: "Być Narodowi użytecznym"

Kończąc obrady prezes Ewa Mańkiewicz-Cudny zaprosiła jego uczestników do kontynuowania tej tematyki podczas XXV Kongresu Techników Polskich, który odbędzie się w czerwcu 2016 r. we Wrocławiu. Pani prezes podziękowała wszystkim prelegentom, uczestnikom, organizatorom i partnerom Forum.

- <http://www.not.org.pl/not/>

XXV Kongres Techników Polskich III Światowy Zjazd Techników Polskich

W dniach 16-18 czerwca 2016 roku we Wrocławiu odbędzie się XXV Kongres Techników Polskich oraz

III Światowy Zjazd Techników Polskich.

Organizatorzy:

Naczelna Organizacja Techniczna Federacja Stowarzyszeń Naukowo-Technicznych, Rada Polskich Inżynierów w Ameryce Północnej, Europejska Federacja Polonijnych Stowarzyszeń Naukowo-Technicznych, Konferencja Rektorów Polskich Uczelni Technicznych, Politechnika Wrocławska, Wrocławska Rada Federacji Stowarzyszeń Naukowo-Technicznych NOT, Akademia Inżynierska w Polsce, Rada Główna Instytutów Badawczych

XXV KONGRES TECHNIKÓW POLSKICH oraz III ŚWIATOWY ZJAZD TECHNIKÓW POLSKICH będą kolejnym wielkim spotkaniem polskich inżynierów zarówno tych mieszkających i pracujących w kraju, jak i poza jego granicami. Ważnym celem inżynierskich zjazdów była i jest integracja środowiska i wymiana wiedzy oraz doświadczeń. Zarówno integracja środowiska technicznego, jak i wymiana doświadczeń i przepływ wiedzy są nam, w dobie globalizacji, potrzebne i dziś. I temu służyć będzie zarówno III SZIP, jak i XXV KTP.

Miejscem integrującym polskich inżynierów niezależnie od miejsca ich zamieszkania i pracy były Zjazdy i Kongresy zwoływane przez stowarzyszenia i organizacje naukowo-techniczne działające w czasie zaborów, II Rzeczypospolitej Polskiej, w PRL oraz w III RP.

W różnych okresach miały różną numerację. Ponieważ stanowią wspólny ciąg działań na rzecz budowy kraju o wysokim poziomie cywilizacyjnym i gospodarczym, w stulecie od zwołania pierwszego Zjazdu (Kraków, 1882r.) postanowiono na Kongresie w 1982r. w Łodzi wprowadzić jedną numerację i nazwę - Kongres Techników Polskich (KTP).

W czasie zaborów

I Zjazd Techników Polskich został zwołany we wrześniu 1882 r. do Krakowa, z inicjatywy Towarzystwa Politechnicznego we Lwowie. Dyskutowano na nim na temat szkolnictwa, terminologii i literatury technicznej oraz potrzeby tworzenia muzealnictwa i ochrony zabytków przemysłowych. II Zjazd (1886 r.) i III Zjazd (1894 r.) odbyły się we Lwowie. Na III Zjeździe powołano Stałą Delegację do Realizacji postanowień Zjazdu. Stworzyło to zaczątki wspólnej organizacji do systematycznej współpracy polskich stowarzyszeń technicznych działających w trzech zaborach.

IV Zjazd obradował w Krakowie (1899 r.), we Lwowie (1910 r.) i ponownie w Krakowie (1912 r.). W tym ostatnim, odbywającym się w formie równolegle obradujących zjazdów branżowych, wzięło udział ponad 550 uczestników, przede wszystkim z zaboru austriackiego i rosyjskiego. VII Zjazd Techników Polskich zwołano w Warszawie w 1917 r. Przewidując bliskie odrodzenie Państwa Polskiego organizatorzy nadali mu nazwę Nadzwyczajnego Zjazdu Techników Polskich. Kończąca uchwała dotyczyła zwołania następnego Zjazdu w Warszawie – stolicy Niepodległego Państwa Polskiego. Pięć miesięcy po VII Zjeździe w Warszawie, Stowarzyszenie Techników Polskich w Rosji zorganizowało Zjazd w Domu Polskim w Moskwie.

II Rzeczpospolita

I Zjazd (VIII KTP) zwołał w 1923 r. Związek Polskich Zrzeszeń Technicznych do Warszawy. Zajmowano się na nim scalaniem odziedziczonych po zaborach systemów gospodarczych. II Zjazd (IX KTP) odbył się w 1927 r. we Lwowie. Głównym tematem jego obrad było przyspieszenie rozwoju gospodarczego Polski. III Zjazd (X KTP) zwołano w 1929 r. do Poznania z okazji odbywającej się Powszechnej Wystawy Krajowej. Przyświecało mu hasło „Program pracy gospodarczej na najbliższe pięciolecie”. Polski Kongres Inżynierów (XI KTP) zwołała w 1937 r. Naczelna Organizacja Inżynierów RP do Lwowa. Przebiegał pod hasłem: „Mobilizacja energii twórczej dla gospodarczego uniezależnienia Polski”. Polski Kongres Techników (XII KTP) odbył się w 1938 r. w Warszawie. Organizatorem była Naczelna Organizacja Stowarzyszeń Techników RP. Obrady obu Kongresów koncentrowały się wokół problemów, takich jak: samorząd techniczny, program przebudowy gospodarczej Polski, kształcenie zawodowe, organizacja przemysłu, rolnictwa i rzemiosła oraz współdziałającej z nimi administracji państwowej.

Okres PRL

I Kongres Techników Polskich (XIII KTP) Naczelna Organizacja Techniczna zwołała do Katowic w grudniu 1946 r. Hasło tego Kongresu brzmiało: „Realizacja Planu Odbudowy – to utrwalać naszych granic, to dobrobyt ogólny”. II Kongres Techników Polskich (XIV KTP) odbył się w 1952 r. w Warszawie. Obrady plenarne toczyły się pod hasłem „Inżynierowie i technicy w szeregach Frontu Narodowego walki o postęp techniczny, pokój i socjalizm”. III Kongres Techników Polskich (XV KTP) również odbył w Warszawie w 1957 r. Obrady toczyły się pod hasłem zapewnienia technice właściwej roli i znaczenia jako podstawowego czynnika rozwoju i postępu gospodarczego w kraju. W obradach uczestniczyło ok. 3 tys. osób. IV Kongres Techników Polskich (XVI KTP) odbył się w 1961 r. we Wrocławiu. Organizatorami Kongresu oprócz NOT były Centralna Rada Związków Zawodowych i Polska Akademia Nauk. Kongres obradował pod hasłem: „Plan 1961-65 - planem modernizacji i rekonstrukcji technicznej”. V Kongres Techników Polskich (XVII KTP) z udziałem 1887 delegatów oraz 593 zaproszonych gości odbył się w 1966 r. w Zabrzu. Dwanaście sekcji problemowych obradowało pod hasłem „Jakość = kadra + technika + organizacja”. VI Kongres Techników Polskich (XVIII KTP) zwołano w 1971 r. do Poznania. Obrady toczyły się na terenie Międzynarodowych Targów Poznańskich pod hasłem „Technika w procesie intensyfikacji gospodarki”. W Kongresie wzięła udział 50 osobowa reprezentacja polskich inżynierów i techników pracujących na obczyźnie, reprezentująca 11 państw. VII Kongres Techników Polskich (XIX KTP) obradował w 1977 r. w Warszawie pod hasłem „Twórczą pracą pomnażamy moc i dobrobyt Ojczyzny”. VIII Kongres Techników Polskich (XX KTP) odbył się w Łodzi w 1982 r. Kongres ten podjął decyzję o wprowadzeniu numeracji nawiązującej do tradycji zjazdów, poczynając od I Zjazdu Techników Polskich w 1882 r. Kongres ten odniósł się do wychodzenia kryzysu gospodarczego. XXI Kongres Techników Polskich zorganizowano w 1987 r. w Gdańsku. W ramach przedkongresowej dyskusji odbyły się ogólnokrajowe narady stowarzyszeń naukowo-technicznych. Kongres przyjął m.in. kodeks etyki zawodowej inżynierów i techników.

25-lat Wolności

XXII Kongres Techników Polskich przebiegał w dwóch sesjach w Warszawie (I sesja w listopadzie 1992 r., sesja II we wrześniu 1993 r.). Ważnym nurtem kongresowej dysku-

sji było rozliczenie działalności NOT w okresie PRL oraz wypracowanie założeń funkcjonowania ruchu stowarzyszeniowego po przemianach ustrojowych. Środowisko techniczne wyraziło zadowolenie z przemian. Jednakże niepokój uczestników budził sposób prywatyzacji dobrych przedsiębiorstw państwowych i deprecjacja dorobku polskich inżynierów. XXIII Kongres Techników Polskich pod hasłem „Technicy bliżej rynku” odbył się również w dwóch sesjach (I sesja w Warszawie w grudniu 2001 r. i II sesja w Poznaniu w czerwcu 2002 r.). W toku branżowych i regionalnych dyskusji wypracowano ponad 200 wniosków i postulatów, które w większości dotyczyły włączenia się środowiska technicznego w dostosowanie polskiej gospodarki do wejścia w strukturę Unii Europejskiej. Za najważniejsze uznano zwiększenie innowacyjności polskiej gospodarki.

XXIV Kongres Techników Polskich. Po 6 latach obecności Polski w Unii Europejskiej środowisko techniczne skupione w NOT uznało za celowe zwołanie Kongresu, który podjął problemy włączania się środowiska technicznego we wdrażanie dorobku nauki do praktyki gospodarczej i współpracy nauka – biznes. Podjął też zagadnienie bezpieczeństwa energetycznego i rozwoju transportu. Kongres został zapoczątkowany na VIII Forum Inżynierskim w czerwcu 2010 r. w Poznaniu, a zakończony Sesją Podsumowującą w Łodzi w maju 2011 r. XXV Kongres Techników Polskich odbędzie się w czerwcu 2016 r. we Wrocławiu, wspólnie z III Światowym Zjazdem Inżynierów Polskich.

- ktp.enot.pl i szip.org.pl

FLIR Systems | Nowe kamery termowizyjne FLIR Vue™ dedykowane do dronów



W ostatnim czasie rynek dronów komercyjnych rozrasta się w gwałtownym tempie, a wraz z nim rośnie zapotrzebowanie na kamery termowizyjne, które będą wykorzystywane w małych bezzałogowych statkach powietrznych. FLIR Vue™ to właśnie odpowiedź FLIR Systems na oczekiwania użytkowników dronów.

W ostatnim czasie rynek dronów komercyjnych rozrasta się w gwałtownym tempie, a wraz z nim rośnie zapotrzebowanie na kamery termowizyjne, które będą wykorzystywane w małych bezzałogowych statkach powietrznych. FLIR Vue™ to właśnie odpowiedź FLIR Systems na oczekiwania użytkowników dronów. Te niewielkie i lekkie urządzenia ważące zaledwie 72 gramy nieznacznie wpływają na wagę i czas lotu drona. Dzięki wykorzystaniu standardowego interfejsu typu power-in/video-out z mini USB oraz zastosowaniu kabli, które są kompatybilne z większością standardowych złączy zasilania i wideo, instalacja kamery jest szybka i prosta. Dodatkowo FLIR Vue™ może być także używany z najpopularniejszymi transponderami wideo i OSD.

Ze względu na swoją specyfikę, bezzałogowe statki powietrzne mogą dostać się do miejsc, do których nie są w stanie dotrzeć pełnowymiarowe statki powietrzne. Sprawia to, że w połączeniu z termowizją ich wykorzystanie jest praktycznie nieograniczone. Technologia obrazowania termowizyjnego wykonywanego z powietrza można m.in. wykorzystać do realizacji następujących działań: poszu-

kiwawczych i ratowniczych, kontroli stacji zasilających, zapewnienia bezpieczeństwa infrastruktury o znaczeniu strategicznym, kontroli rurociągów i przewodów elektrycznych, działań związanych z reagowaniem kryzysowym, monitorowania żywego inwentarza oraz w rolnictwie.

FLIR Vue™ to najlepsze w swojej klasie kamery termowizyjne oparte na technologii „Plug&Play”, które obecnie dostępne są już w cenie 1 499 Euro za kamerę o rozdzielczości 336×256 oraz w cenie 2 999 Euro za kamerę o rozdzielczości 640×480. Łatwa integracja, małe rozmiary i niewielka waga oraz przystępna cena to krótka charakterystyka FLIR Vue™.

Więcej na: www.linc.pl oraz www.flir-termowizja.pl

Autor - Linc Polska Sp. z o.o.

Zasada *in dubio pro tributario* nie może być "martwym" przepisem

Rzecznik Praw Obywatelskich spotkał się z członkiem zarządu Federacji MSP Markiem Isańskim i wyraził swoje poparcie dla działań zmierzających do stosowania zasady *in dubio pro tributario* w praktyce.

Głównym tematem spotkania była poważna obawa polskich przedsiębiorców, że wprowadzona do Ordynacji podatkowej zasada o rozstrzyganiu wątpliwości co do treści przepisów prawa podatkowego na korzyść podatnika zostanie przepisem "martwym". Minister finansów nie przeprowadził odpowiednich szkoleń aparatu skarbowego, mających na celu właściwe zrozumienie i wdrożenie tej zasady. Zdaniem Marka Isańskiego, za zmianą przepisów powinna iść zmiana wieloletnich nawyków i przyzwyczajeń urzędników.

Stosowanie zasady *in dubio pro tributario* stanowi gwarancję przestrzegania podstawowego prawa każdego podatnika, jakim jest pewność co do tego, jaki podatek na nim ciąży. Rzecznik Praw Obywatelskich podzielił obawy środowiska przedsiębiorców i uznał sprawę za ważną dla przestrzegania praw obywatelskich, a także zapowiedział, że bezzwłocznie przygotuje opracowanie-broszurę o prawach obywatela wynikających z uchwalenia zasady *in dubio pro tributario*. Dokument będzie dostępny m.in. na stronie internetowej RPO.

Ponadto, Rzecznik wystąpi do ministra finansów o informację na temat podjętych działań organizacyjnych wynikających z konieczności stosowania tejże zasady przez aparat skarbowy. Zorganizuje również seminarium z udziałem sędziów NSA, ministra finansów i prawników, aby ta zasada w sposób jak najbardziej efektywny chroniła prawa obywateli-podatników.

5 sierpnia br. Sejm uchwalił zmianę ustawy Ordynacja podatkowa, wprowadzającą zasadę nakazującą rozstrzygać wątpliwości co do treści przepisów podatkowych na korzyść podatników. Do ostatniej chwili toczona była walka przez ministra finansów o zmianę treści przepisu na zdecydowanie mniej korzystną dla podatników, a w zasadzie chodziło o wprowadzenie przepisu dającego jedynie pozorną korzyść dla podatnika. Federacja MSP, jako strona inspirująca prezydencki projekt nowelizacji, opowiadała się za pierwotnym jego brzmieniem i ostatecznie w takiej formie został on uchwalony.

- Redakcja portalu MSP-24

Pierwsza runda Alpol Bowling CUP za nami

W piątek 30 października zakończyła się pierwsza runda turnieju Alpol Bowling CUP. Rywalizowało w niej 350 zawodników z 42 drużyn.

Ostatnie rozgrywki w I rundzie rozegrano w Warszawie i Wrocławiu. Dotychczasowy lider rozgrywek, drużyna „Zawisza Bowling Team” z Bydgoszczy, ustąpiła miejsce drużynie „Warsaw Hawks” z Warszawy – Mokotowa, która uzyskała wynik 2941 punktów. Tym samym padł tam rekord strik’ów - 47.



Zawodnicy z Sopotu



Zawodnicy z Warszawy

Złotym Partnerem turnieju została firma Honeywell. Patronem honorowym - Polska Izba Systemów Alarmowych, fundator nagrody specjalnej dla uczestnika turnieju, który zdobył największą liczbę strik’ów we wszystkich trzech rundach. Fundatorem części nagród stało się Stowarzyszenie POLALARM. Turniej odnotował również licznych patronów medialnych i zarazem stał się największym wydarzeniem w branży elektrycznych systemów zabezpieczeń.



Dyrektor regionu południe Pan Marcin Gierszner tłumaczy zasady bowlingu



OGÓLNOPOLSKI TURNIEJ BRANŻOWY



6

listopada (piątek) rozpoczęła się II runda turnieju. Zmierzyły się w niej drużyny „Minionków” oraz „Dzikich Kotów” z Bielska - Białej oraz drużyny „Zawisza Bowling Team” i „Fireball” z Bydgoszczy. Zawodnikom życzymy sukcesów i dobrej rywalizacji.



- inf. Alpol

Targi, Wystawy, Konferencje

Targi ochrony budynków i bezpieczeństwa Perimeter Protection 2016

12 – 14 stycznia 2016 r., Norynbergia

www.targiwniemcech.pl

XVI Targi ELEKTROTECHNIKA 2016

27 – 29 stycznia 2016 EXPO XXI, Warszawa

www.elektroinstalacje.pl

INTERSEC

17 - 19 stycznia 2016 r, Dubaj

Intersec to jedno z najważniejszych międzynarodowych targów bezpieczeństwa, ochrony i ratownictwa.

www.intersecexpo.com, www.targifrankfurt.pl

BUDMA

Międzynarodowe Targi Budownictwa i Architektury

2 – 5 lutego 2016 r., Poznań

www.budma.pl/pl

IX Międzynarodowa Konferencja i Wystawa Lotnisko 4 lutego 2016 r., Warszawa

www.lotnisko.ztw.pl

Targi WARSAW HOME

26 – 28 lutego 2016, Nadarzyn

www.targi-polska.pl

Targi Budownictwa, Instalacji i Wyposażenia Wnętrz 2016

26 - 28.02.2016, Gliwice

www.promocja-targi.pl

Targi Inwestycyjne Invest-Tor 2016

5 – 6 marca 2016, Toruń

www.targi-polska.pl

SECUTECH INDIA

marzec 2016 r., Mumbai

www.secutechindia.co.in, www.targifrankfurt.pl

Light + Building

13 – 18 marca 2016 r., Frankfurt

www.targifrankfurt.pl

SIBEX 2016 Targi Budowlane

1 - 3 kwietnia 2016, Sosnowiec

www.exposilesia.pl

EXOP Dom Podkarpackie Targi Budownictwa, Wyposażenia Wnętrz i Ogrodów

8 – 10.04.2016, Rzeszów

www.targi-polska.pl

II Targi Budowlane BOM i OTOCZENIE BUDOWNICTWO, INSTALACJE, WNĘTRZA

9 – 10.04.2016, Katowice

www.promocja-targi.pl

49 Międzynarodowe Targi Budownictwa i Wyposażenia Wnętrz TWÓJ DOM 2016

15 – 17 kwietnia 2015, Bielsko-Biała

www.targi-polska.pl



25 – 28 kwietnia 2016 r., Poznań

www.securex.pl/pl

MIPS

**Targi Bezpieczeństwa, Zabezpieczeń
i Ochrony Przeciwpowodzi**

04.2016, Rosja, Moskwa

www.sawo.pl

**HANNOVER MESSE
Międzynarodowe Targi Przemysłowe**

Niemcy, Hanower 25-29.04.2016

www.sawo.pl

SAWO

**Międzynarodowe Targi Ochrony Pracy,
Pożarnictwa i Ratownictwa**

28 – 29 kwietnia 2016 r., Poznań

www.sawo.mtp.pl/pl

**XXI Podhalańskie Targi Budownictwa,
Instalacji, Wnętrz Nowy Targ**

7 – 8 maja 2016, Nowy Targ

www.targi-polska.pl

IV Targi Logistyki Służb Mundurowych TLSM

10 – 11.05.2016, Łódź

www.targi-polska.pl

TOS+H EXPO

Targi Bezpieczeństwa i Higieny Pracy

8 - 11.05.2016, Turcja, Stambuł

www.sawo.pl

**Targi Przemysłu Obronnego KADEX'2016
Kazakhstan Defence Expo**

2 – 5 czerwca 2016, Kazachstan – Astana

<http://kadex.kz/new/?lang=en>

EDURA

**XI Międzynarodowa Wystawa Ratownictwa
i Technika Przeciwpowodzi**

9 – 11 czerwca 2016 r., Kielce

www.targikielce.pl/pl/edura.htm

**XIV edycja Bałtyckich Targów Militarnych
BALT-MILITARY-EXPO**

20 - 22 czerwca 2016 r.

**Centrum Wystawienniczo-Kongresowe
AMBEREXPO Gdańsk**

www.baltmilitary.amberexpo.pl

MSPO

XXIV Międzynarodowy Salon Przemysłu Obronnego

6- 9.09.2016, Kielce

www.targikielce.pl

INTERSEC

7 – 9 września 2016 r., Buenos Aires, Argentina

www.intersecbuenosaires.com.ar, www.targifrankfurt.pl

PROTECTION TECHNOLOGIES

**Targi Nowoczesnych Technologii w zakresie
Ochrony, Bezpieczeństwa i Ratownictwa**

09.2016, Ukraina, Kijów

www.sawo.pl

ARMS & SECURITY

Targi Wyposażenia dla Wojska i Policji

09.2016, Ukraina, Kijów

www.sawo.pl

LOKUM EXPO

Salon Obsługi i Utrzymania Nieruchomości

18 – 20.10.2016 r.

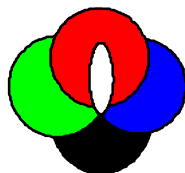
www.targikielce.pl

EXPOPROTECTION

**Międzynarodowe Targi Zarządzania Ryzykiem,
Zabezpieczeń, Bezpieczeństwa Pracy,
Ochrony Przeciwpowodzi, Zagrożeń Przemysłowych
i Środowiska Naturalnego**

7 - 9.11.2016, Francja, Paryż

www.sawo.pl



Ogólnopolskie Stowarzyszenie Inżynierów i Techników
Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem
„POLALARM”

zaprasza producentów oraz dystrybutorów elektronicznych i elektromechanicznych
urządzeń oraz systemów przeznaczonych do ochrony osób i mienia, do udziału w

XVI edycji Konkursu

POLSKI MISTRZ TECHNIKI ALARMOWEJ 2016

im. Włodzimierza Kuczkowskiego

Zgłoszenia do udziału w Konkursie będą przyjmowane do dnia 31 stycznia 2016 roku na drukach *Wniosku o udział w Konkursie*. Wypełniony *Wniosek* (wraz z załącznikami) należy przesłać na adres Biura Zarządu Stowarzyszenia „POLALARM”: ul. Nowogrodzka 18 lok. 8, 00-511 Warszawa, e-mail: polalarm@polalarm.com.pl

Przyznanie tytułów, nagród i wyróżnień w Konkursie nastąpi do dnia 3 marca, a uroczystość wręczenia nagród Laureatom odbędzie się w pierwszym dniu Międzynarodowej Wystawy Zabezpieczeń „SECUREX 2016”. tj. 25 kwietnia 2016 roku na terenie Międzynarodowych Targów Poznańskich.

Na stoisku Stowarzyszenia na SECUREX 2016 prezentować będziemy urządzenia i systemy, które zajęły I miejsce w grupie oraz Laureata Głównej Nagrody "Złota Zbroja". W miarę możliwości postaramy się zaprezentować wszystkie produkty zgłoszone do Konkursu. Wszyscy Uczestnicy Konkursu będą mieli możliwość umieszczenia na naszym stoisku ulotek i folderów reklamowych z informacją o zgłoszonych do Konkursu wyrobach oraz zorganizowania krótkich prezentacji swoich wyrobów zaproszonym przez siebie gościom.

Regulamin Konkursu oraz *Wniosek o udział w Konkursie* zamieszczone są na stronie www.polalarm.org

Bliższych informacji na temat Konkursu udziela Biuro Zarządu Stowarzyszenia „POLALARM”, tel. 22 626 90 31, 22 625 57 43, e-mail: polalarm@polalarm.com.pl

Serdecznie zapraszamy do udziału w Konkursie

POLSKI MISTRZ TECHNIKI ALARMOWEJ 2016 !