

PAWEŁ PAJORSKI

Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego
„Apeiron” w Krakowie

SYSTEMY ZABEZPIECZENIA TECHNICZNEGO W SŁUŻBIE OCHRONY OSÓB

TECHNICAL SECURITY SYSTEMS IN THE SERVICE
OF PROTECTION OF PEOPLE ACTIVITIES

ABSTRACT

The author of this article presents issue of technical security (technological protection systems) to protect people. Discussed a safe room, technical, electronic devices and systems signaling threats of persons protected, secure residence (building and the adjacent protected area).

KEY ACCOUNT

technical security, protection of people, security, threats

ABSTRAKT

Autor niniejszego artykułu przedstawia zagadnienie zabezpieczenia technicznego (systemów zabezpieczenia technicznego) w ochronie osób. Omówione zostały pomieszczenia bezpieczne, techniczne elektroniczne urządzenia i systemy sygnalizujące zagrożenia chronionych osób, zabezpieczenia rezydencji (obiektu wraz z przyległym obszarem chronionym).

SŁOWA KLUCZOWE

zabezpieczenia techniczne, ochrona osób, bezpieczeństwo, zagrożenia

Ochronę osobistą, zwaną z języka angielskiego CP¹, większość ludzi kojarzy wyłącznie z kilkoma roslymi, dobrze zbudowanymi mężczyznami poruszającymi się w jakimś określonym szyku przy osobie ochraniającej. Takie zawężenie ochrony osobistej do eskorty pieszej (bo o niej tu mowa), a tylko czasami rozbudowanej o eskortę samochodową, jest niestety błędne. Jak wynika z zapisu w ustawie², ochrona osób to działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej³, czyli bardzo szerokie spektrum działań ochronnych. Zadania te realizuje, ze względu na ich niekiedy bardzo skomplikowaną materię, cały sztab ludzi planujących operacje oraz przedsięwzięcia ochronne i wykonujących szereg zadań, które często nie kojarzą się w ogóle z działaniami ochronnymi w ochronie osób.

O ludziach dbających o bezpieczeństwo ochraniających osób, powiedziano już wiele. Bodyguardzi⁴, ochroniarze, goryle⁵, bo tak najczęściej się o nich mówi są wdzięcznym tematem filmów, rozmów i opracowań zarówno tych popularno naukowych jaki i, w pełnym tego słowa znaczeniu, naukowych. Wobec tego autor niniejszego opracowania postanowił skupić się na zagadnieniu zabezpieczenia technicznego (systemów zabezpieczenia technicznego) w ochronie osób.

W skład ochrony technicznej wchodzi: elektroniczne urządzenia i systemy sygnalizujące zagrożenia chronionych osób (elektroniczne systemy alarmowe), systemy monitorujące te zagrożenia, systemy ograniczające i opóźniające dostęp lub wtargnięcie na jakiś chroniony obszar (urządzenia i środki mechanicznego zabezpieczenia)⁶, teren lub obiekt.

¹ CP – skrót od ang. Close Protection, a właściwie Close Personal Protection – ochrona bezpośrednia.

² Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2014 r. Nr 0, poz. 1099).

³ Ibidem, art. 2, pkt. 4.

⁴ Bodyguard (ang.) - dosłownie: „Strażnik Ciała” – osoba, która własnym ciałem zasłoni, w razie potrzeby, osobę ochraniającą – pracownik ochrony fizycznej osób. (por. K. Chmielarz, *Bodyguard*, TOSW „SKORPION”, Tarnów 1999, ISBN: 83-912562-0-0, s. 39).

⁵ Goryl - nazwa pochodzi od „Les Gorilles” (Goryle) czyli członków ochrony osobistej gen. Ch. de Gaulle’a. Przyjęła się jako zwyczajowa nazwa członków ochrony osobistej na całym świecie.

⁶ Por. ustawa z dnia 22 sierpnia 1997 r. o ochronie osób..., op. cit., art. 3 ust. 2.

Do systemów sygnalizacji zagrożeń zaliczamy m. in.:

1. systemy sygnalizacji włamania i napadu (SSWiN);
2. systemy sygnalizacji (alarmowania) pożarowej (SSP/SAP);
3. systemy lokalizacji pojazdów;
4. systemy lokalizacji osób;
5. systemy telewizji przemysłowej zwane też systemami telewizji dozоровej lub obserwacyjnej (CCTV, TVD, TVO), a czasami monitoringiem wizyjnym;
6. systemy kontroli dostępu (KD, ACC).

Do systemów monitorujących i rejestrujących zaliczamy:

1. systemy telewizji przemysłowej (CCTV);
2. systemy lokalizacji pojazdów;
3. systemy lokalizacji osób;
4. stacje monitorowania obiektów (SMO);
5. systemy kontroli dostępu;
a ostatnimi czasy także:
6. mobilne systemy nadzoru wizyjnego.

Do urządzeń i systemów ograniczających i opóźniających dostęp lub wtargnięcie zaliczamy:

1. płoty, zapory, blokady, ogrodzenia;
2. drzwi, okna, szyby, rolety, kraty;
3. ściany, stropy;
4. pomieszczenia specjalne (tzw. pomieszczenia bezpieczne);
5. systemy zadymiające, ogłuszające, odstrasające, obezwładniające;
6. zamki, zasuw, zapory itp.

Wśród najczęściej stosowanych spotyka się:

1. w zakresie elektronicznej ochrony przed włamaniem i napadem:
 - systemy ochrony peryferyjnej, } systemy ochrony zewnętrznej
 - systemy ochrony obwodowej, }
 - systemy ochrony wewnętrznej.
2. w zakresie elektronicznej ochrony przed pożarem:
 - systemy alarmowania (sygnalizacji) pożarowego,
 - systemy gaszenia,
 - systemy oddymiania.
3. w zakresie elektronicznej ochrony przed porwaniem (uprowadzeniem):
 - systemy lokalizacji pojazdu,
 - systemy lokalizacji osoby.

4. w zakresie elektronicznego nadzoru i kontroli pracowników ochrony odpowiedzialnych za bezpieczeństwo obiektu:

- system sygnalizacji pozycji horyzontalnej,
- system lokalizacji pojazdu,
- system lokalizacji osoby,
- system kontroli pracy wartowników.

Są to systemy najczęściej stosowane w ochronie osób, jednakże czasami stosuje się także systemy bardziej specjalistyczne.

Autor nie wspominał tu o budowlanych urządzeniach zabezpieczających (choć niektóre z nich wymienił z nazwy), stanowiących środki zabezpieczenia utrudniające (opóźniające) dostęp do chronionego obiektu lub osób, będące elementami konstrukcyjnymi obiektu. Nie zostały one wymienione, gdyż wydaje się być oczywistym zaliczenie do nich ścian, stropów, drzwi, krat, rolet, okiennic, okien, szyb itp.

Wielu z czytelników nurtuje zapewne pytanie, co to ma wspólnego z ochroną osób? Wbrew pozorom – bardzo wiele. Począwszy od ochrony peryferyjnej rezydencji, na pomieszczeniu bezpiecznym skończywszy. Zacznijmy może od końca, od zdefiniowania pojęcia: „pomieszczenie bezpieczne”. Co to jest takiego „pomieszczenie bezpieczne” i czym się charakteryzuje?

Pomieszczenie bezpieczne⁷ to takie pomieszczenie, w którym osoba ochraniana wraz z najbliższymi jej osobami (lub członkami najbliższego otoczenia) i ewentualnie ich bezpośrednią ochroną, może przetrwać zamach bezpośredni i w miarę bezpiecznie doczekać się rozwiązania kryzysu⁸. Przyjmuje się, że pomieszczenie bezpieczne powinno zapewnić 30- 60 minutową odporność na włamanie.

Najczęściej jest to pomieszczenie adaptowane, ze zwykłego pomieszczenia o innym przeznaczeniu, na pomieszczenie bezpieczne. Rzadziej budowane jest specjalne pomieszczenie od początku dedykowane temu celowi.

Czym się charakteryzuje pomieszczenie adaptowane? Powinno posiadać solidne ściany i stropy oraz drzwi i okna o podwyższonej odporności na włamanie, które dodatkowo wyposażone są w blokadę otwarcia od środka (nie ma możliwości ich otwarcia z zewnątrz, nawet w przypad-

⁷ Por. P. Consterdine, *The modern Bodyguard. The manual of close protection training*, Summersdale, Leeds 2000, ISBN 09-53763-81-1, s. 68.

⁸ Por. P. Consterdine, *Poradnik współczesnego bodyguarda. Nowoczesna ochrona*, Wydawnictwo Bellona, Warszawa 2009, ISBN 978-83-111144-5-6, s. 83.

ku posiadania oryginalnego klucza). Pomieszczenie adaptowane powinno być również wyposażone w środki łączności telefonicznej i radiowej, apteczkę pierwszej pomocy przedmedycznej, podręczne środki przeciwpożarowe, latarkę, radioodbiornik i środki ochrony górnych dróg oddechowych oraz co najmniej przycisk napadowy, a także odpowiedni zapas wody pitnej. Pomieszczenie, jak już wcześniej wspomniano, powinno zapewnić odporność na włamanie przez około 30-60 minut oraz powinno posiadać drogę ewakuacji.

Czym charakteryzuje się pomieszczenie dedykowane na cele pomieszczenia bezpiecznego? Winno ono posiadać solidne ściany i stropy, najlepiej gdyby nie miało okien lub, jeżeli ma okna to zarówno szyby jak i cała „stolarka” okienna powinna posiadać odpowiednią do zagrożenia klasę kuloodporności lub wręcz odporności na detonację. Okno winno być osadzone na stałe w futrynie okiennej (nie otwierane) jednakże, o ile ma służyć jako wyjście awaryjne, winno posiadać system jego otwarcia od środka.

Wejście do pomieszczenia powinno posiadać drzwi w odpowiedniej do stopnia zagrożenia klasie odporności na włamanie z mechaniczną blokadą wewnętrzną (nawet w sytuacji, gdy funkcjonuje blokada elektroniczna). Futryny powinny być głęboko zakotwione w ścianach w sposób uniemożliwiający ich wyjęcie bez użycia materiałów wybuchowych lub specjalistycznego sprzętu budowlanego. Pomieszczenie takie powinno być dodatkowo wyposażone w środki łączności umożliwiające kontakt z ochroną jak i instytucjami zewnętrznymi oraz służbami ratunkowymi (Policja, Straż Pożarna, Pogotowie Ratunkowe, wewnętrzne służby ochrony, agencja ochrony). Powinno również mieć zainstalowany niezależny system alarmowy (sygnalizacji włamania i napadu, sygnalizacji pożarowej, kontroli dostępu, telewizji dozorowej). Przy czym system SWiN zapewnia również przekazanie sygnału alarmu napadowego do Centrum Monitorowania Obiektów, należącego do firmy realizującej usługę monitoringu, ewentualnie także do Lokalnej Stacji Monitorowania Obiektu zlokalizowanej na jego terenie lub w bezpośrednim sąsiedztwie. System telewizji dozorowej (CCTV) winien umożliwiać obserwację podejścia do pomieszczenia bezpiecznego z jego wnętrza, jak również zapewnić obserwację ewentualnych dróg ewakuacyjnych.

Pomieszczenie takie, winno też być zaopatrzone w podręczne środki gaśnicze, oświetlenie awaryjne, telefon komórkowy, latarkę (najlepiej kilka, wraz

z zapasowymi bateriami), apteczkę pierwszej pomocy przedmedycznej (najlepiej z automatycznym defibrylatorem zewnętrznym) oraz podstawowe środki medyczne, w skład których wchodzi niezbędne leki przyjmowane zarówno przez osobę ochraniającą jak i członków jej najbliższego otoczenia. Warto też zabezpieczyć odpowiednią ilość wody pitnej oraz podlegające długiemu przechowywaniu podstawowe produkty spożywcze. Niezbędnym wyposażeniem są również środki ochrony górnych dróg oddechowych. W przypadku pomieszczenia dedykowanego można rozważyć maskowanie wejścia, filtrację powietrza itp.

Omówione zostało pomieszczenie bezpieczne, zatem można przejść do ogólnego zabezpieczenia rezydencji (obiektu wraz z przyległym obszarem chronionym).

Obiekt winien posiadać ochronę peryferyjną tzn. odpowiednie ogrodzenie, tak skonstruowane, aby w sposób znaczny utrudniać jego pokonanie. Teren podejścia do ogrodzenia winien być monitorowany systemem CCTV. Samo ogrodzenie winno być zabezpieczone systemem kontroli dostępu i sygnalizacji włamania adekwatnym do rodzaju ogrodzenia, który umożliwi transmisję sygnału alarmowego w przypadku prób sforsowania ogrodzenia. System winien zapewniać przekaz informacji o otwarciu wszystkich bram, furtek, śluz, wjazdów, przejść itp. Brama wjazdowa na teren rezydencji winna być tak skonstruowana, aby w poważnym stopniu utrudnić jej sforsowanie przy użyciu pojazdu lub podjazd do niej winien być zabezpieczony specjalnym systemem wysuwanych kolców, słupów lub innych szykan uniemożliwiających jej sforsowanie pojazdem. Teren pomiędzy ogrodzeniem, a samym budynkiem zajmowanym przez osobę ochraniającą, winien być monitorowany przy zastosowaniu systemu CCTV. W przypadku obszarów rozległych można rozważyć wykorzystanie mobilnych systemów nadzoru wizyjnego posadowionych na bezzałogowych platformach latających⁹ (dron) lub bezzałogowych platformach kołowych bądź gąsienicowych. W przypadku znacznych obszarów (zbiorników) wodnych należy rozważyć także możliwość wykorzystania platform pływających bądź podwodnych.

⁹ Bezzałogowa platforma latająca to bezpilotowy statek powietrzny zwany także bezzałogowym statkiem latającym sterowany zdalnie, manualnie, półautomatycznie, a także platformy autonomiczne lub stanowiące kombinację powyższych rozwiązań (cf.: M. Kędziński, A. Fryśkowska, D. Wierzbicki, *Opracowania fotogrametryczne z niskiego pułapu*, WAT, Warszawa 2014, ISBN 978-83-7938-047-3, s. 9; a także: T. Zieliński, *Funkcjonowanie bezzałogowych systemów powietrznych w sferze cywilnej*, SILVA RERUM, Poznań 2014, ISBN: 978-83-64447-31-0, s. 33).

Sam budynek winien posiadać system ochrony obwodowej strefy zewnętrznej przy użyciu systemów SWiN oraz CCTV, przy czym system SWiN winien być tak skonfigurowany aby możliwe było jego uzbrojenie w trakcie pobytu jego mieszkańców wewnątrz domu oraz, aby możliwy był obchód obiektu, dokonywany przez pracowników ochrony, bez potrzeby naruszania stref chronionych. Ponadto budynek powinien być wyposażony w niezależne systemy SWiN i SAP oraz, o ile to możliwe, ekonomicznie uzasadniony system gaszenia. System SWiN winien być tak skonfigurowany, aby umożliwiał ochronę wybranych stref, czy też poszczególnych pomieszczeń, pomimo pobytu w nich domowników. W skład takich systemów powinny wchodzić m. in. czujki dualne PIR¹⁰ oraz MW¹¹, czujki z funkcją antymasking¹² oraz bariery podczerwieni lub bariery mikrofalowe. Oczywiście nie wyklucza to zastosowania innych czujek, dobranych odpowiednio zarówno do charakteru i przeznaczenia chronionego pomieszczenia jak i strefy czy rodzaju zagrożenia. Wszystkie systemy sygnalizacji zagrożeń winny być na bieżąco monitorowane przez co najmniej dwie stacje monitorowania obiektów¹³, główną i zapasową. Obie stacje mogą być lokalnymi stacjami monitorowania, a więc opartymi na obsłudze stanowiącej etatową ochronę fizyczną obiektu, jednakże oddalonymi od siebie (zlokalizowanymi w różnych budynkach). Stacja zapasowa może być albo w „uśpieniu” tzn. rejestrować przychodzące sygnały, ale ich nie obsługiwać (z możliwością, natychmiastowego przejęcia wszystkich funkcji stacji głównej), albo być stacją aktywną potwierdzającą każdorazowo do stacji głównej odebrany sygnał.

¹⁰ PIR (ang. *Passive Infra Red*) – pasywny czujnik podczerwieni, służący do wykrywania ruchu. Stosowany w systemach alarmowych, systemach automatycznego załączania oświetlenia i wentylacji itp.

¹¹ MW (ang. *Microwave Detectors*) – czujnik alarmowy, który stosuje detekcję mikrofalową. Detektory tego typu do wykrywania poruszających się obiektów wykorzystują zjawisko fal elektromagnetycznych, zaś sama detekcja opiera się na zjawisku Dopplera.

¹² Antymasking zabezpiecza czujkę przed zasłonięciem, działa 24 godziny na dobę, przez 7 dni w tygodniu, także wtedy, kiedy system alarmowy jest wyłączony (nieuzbrojony). Po zasłonięciu czujki natychmiast generowany jest alarm.

¹³ Stacja monitorowania obiektów (SMO) – uzbrojone stanowisko interwencyjne (USI) – na podstawie § 1 pkt. 2, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji (Dz.U. 2015 Nr 0 poz. 992), co najmniej jednego uzbrojonego pracownika ochrony, który po uzyskaniu informacji z urządzeń lub systemów alarmowych sygnalizujących zagrożenie podejmuje decyzję o rodzaju środków niezbędnych do jego usunięcia.

Innym rozwiązaniem może też być zlokalizowanie stacji głównej na terenie chronionej posesji, a funkcję stacji zapasowej może spełniać wtedy Stacja Monitorowania Obiektów rodzimej firmy obsługującej całość kontraktu na usługę ochronną lub też innej firmy specjalizującej się w usługach monitorowania z reakcją zmotoryzowanych patroli kontrolno-interwencyjnych (Grup Interwencyjnych¹⁴). Niezaprzeczalnym atutem własnej SMO jest większy stopień poufności i ochrony informacji, niż korzystanie z „obcej” SMO.

Poza systemami sygnalizacji zagrożeń oraz systemami monitorowania i rejestracji, budynek powinien być wyposażony w systemy ograniczające i opóźniające dostęp osób niepowołanych. Powinny to być przynajmniej:

- szyby o podwyższonej odporności na stłuczenie,
- drzwi i okna o podwyższonej odporności na włamanie,
- zamki patentowe.

Oczywistym jest, że zabezpieczenia te będą coraz wyższej klasy (odporniejsze na różne formy ich forsowania), w zależności od stopnia zagrożenia osób ochraniających, lub jak kto woli, od ich subiektywnego poczucia bezpieczeństwa.

Systemy te w stosunku do osób ochraniających uzupełniamy o systemy indywidualnej lokalizacji i alarmowania. Systemy takie oparte najczęściej na GPS¹⁵ lub GSM¹⁶ umożliwiają zwiększenie prawdopodobieństwa skutecznej ochrony przed porwaniem (uprowadzeniem) i umożliwiają ewentualne szybsze odbicie osoby uprowadzonej przez stosowne służby.

Ważnym elementem ochrony technicznej są systemy przeznaczone do kontroli i monitorowania pracowników ochrony.

¹⁴ Grupa interwencyjna – na podstawie § 1 pkt 3, rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji (Dz.U. 2015 Nr 0 poz. 992), co najmniej dwóch uzbrojonych pracowników ochrony, którzy po uzyskaniu za pośrednictwem uzbrojonego stanowiska interwencyjnego informacji z urzędzeń lub systemów alarmowych sygnalizujących zagrożenie chronionych osób lub mienia wspólnie realizują zadania ochrony osób lub mienia w formie bezpośredniej ochrony fizycznej doraźnej na terenie chronionego obszaru, obiektu lub urzędnika.

¹⁵ GPS (ang. *Global Positioning System*) – system nawigacji satelitarnej, stworzony przez Departament Obrony Stanów Zjednoczonych, obejmujący swoim zasięgiem całą kulę ziemską.

¹⁶ GSM (ang. *Global System for Mobile Communications*) – Światowy System Komunikacji Mobilnej, najczęściej wykorzystywany system telefonii komórkowej na całym świecie, znany również jako 2G (telefonii komórkowa drugiej generacji).

Jak już wspomniano na początku tego tekstu, są to urządzenia i systemy:

1. Sygnalizacji bezruchu (PSSS – *No Movement i Man Down*);
2. System lokalizacji osoby (RTLS);
3. System kontroli pracy wartowników.

Wszystkie trzy systemy nie chronią w pełnym tego słowa znaczeniu, a jedynie zwiększają prawdopodobieństwo natychmiastowej reakcji pozostałych pracowników ochrony na zasygnalizowane zagrożenie. Przeznaczenie oraz zadanie każdego z tych systemów wydaje się być oczywiste.

Pojazdy to kolejny środek ochrony technicznej osoby ochranianej. Dobry opancerzony lub pancerny samochód stanowić może ruchome „pomieszczenie bezpieczne”. Poza dobrym opancerzeniem, w odpowiedniej klasie w stosunku do potencjalnego zagrożenia, pojazd powinien być wyposażony w system lokalizacji pojazdu umożliwiający nie tylko wskazanie aktualnego miejsca znajdowania się pojazdu, ale również wezwanie pomocy czy też zdalne unieruchomienie pojazdu. Bardziej ekstrawaganckie pojazdy tej kategorii posiadają jeszcze niezależny zespół filtracji powietrza zasilającego wnętrze pojazdu lub wręcz zespół butli tlenowych zasilających jego wnętrze.

Przedstawiony powyżej zarys środków zabezpieczenia technicznego (ochrony technicznej) w ochronie osób jest niestety często tylko życzeniem. Większość osób ochranianych albo nie wymaga takiego nakładu sił i środków do zapewnienia im bezpieczeństwa, albo nie widzi potrzeby wydawania aż tak dużych pieniędzy na utrzymywanie swojego bezpieczeństwa. Jednakże zawsze warto wiedzieć, co można zaoferować osobie ochranianej w celu realizacji procedur zmierzających do utrzymania czy nawet podniesienia jej bezpieczeństwa.

BIBLIOGRAFIA

Wydawnictwa zwarte

1. Chmielarz K., *Bodyguard*, TOSW „SKORPION”, Tarnów 1999, ISBN: 83-912562-0-0.
2. Consterdine P., *Poradnik współczesnego bodyguarda. Nowoczesna ochrona*, Wydawnictwo Bellona, Warszawa 2009, ISBN 978-83-111144-5-6.
3. Consterdine P., *The modern Bodyguard. The manual of close protection training*, Summersdale, Leeds 2000, ISBN 09-53763-81-1.
4. Kędzierski M., Fryškowska A, Wierzbicki D., *Opracowania fotogrametryczne z niskiego pułapu*, WAT, Warszawa 2014, ISBN 978-83-7938-047-3.
5. Zieliński T., *Funkcjonowanie bezzatogowych systemów powietrznych w sferze cywilnej*, SILVA RERUM, Poznań 2014, ISBN: 978-83-64447-31-0.

Akty prawne

6. Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2014 r. Nr 0, poz. 1099).
7. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 21 października 2011 r. w sprawie zasad uzbrojenia specjalistycznych uzbrojonych formacji ochronnych i warunków przechowywania oraz ewidencjonowania broni i amunicji (Dz.U. 2015 Nr 0 poz. 992).