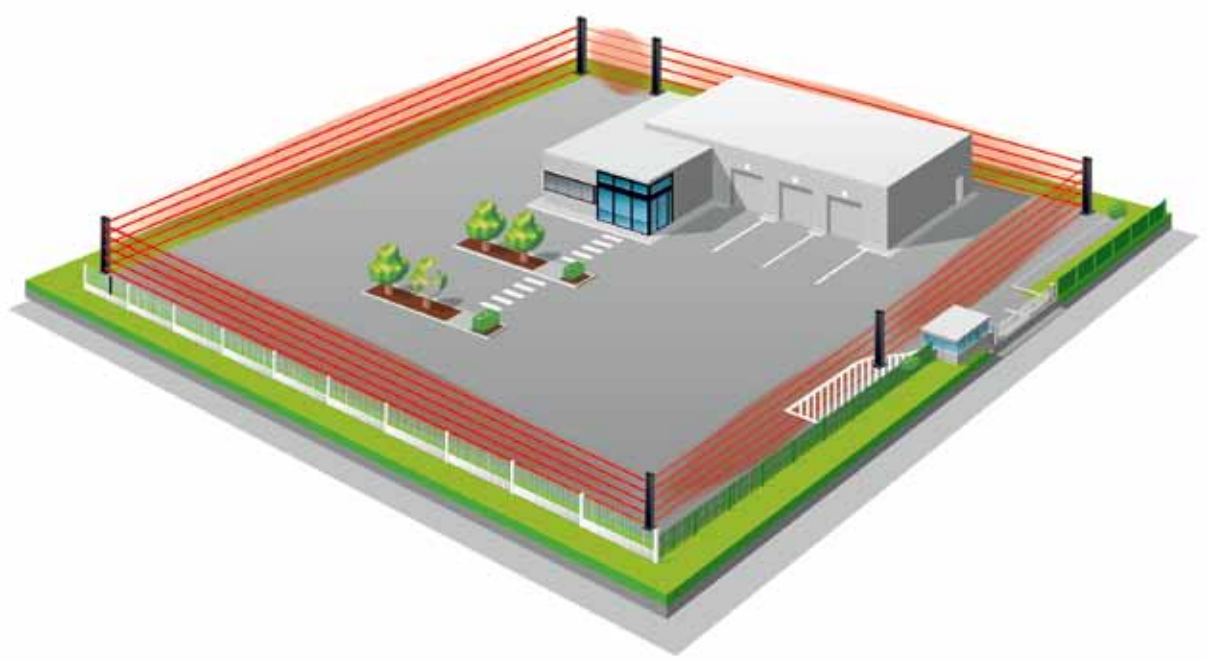
PODSTAWY ZABEZPIECZANIA OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ



Zrozumienie niektórych zapisów **Narodowego Programu Ochrony Infrastruktury Krytycznej 2015** (NPOIK 2015) może wymagać poznania podstaw prawidłowego zabezpieczania obiektów. W Załączniku 1 pt. „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje" napisano: „W celu zapewnienia efektywności systemu bezpieczeństwa fizycznego dobrą praktyką jest podział terenu, na którym zlokalizowana jest IK (infrastruktura krytyczna – przyp. Redakcji), na strefy ochrony i zaprojektowanie ich zgodnie z zasadą ochrony w głąb (ochrona powłokowa). Niekiedy wyróżnia się także strefę zewnętrzną poza obiektem. Każda ze stref musi być zaprojektowana w celu maksymalnego spowolnienia działań potencjalnego napastnika, a natężenie sił i środków ochrony powinno rosnąć w miarę zbliżania się potencjalnych napastników do strefy chroniącej kluczowe elementy infrastruktury organizacji. W rezultacie zniechęci to napastnika lub da więcej czasu na adekwatną do zagrożenia odpowiedź systemu ochrony lub wykwalifikowaną pomoc.

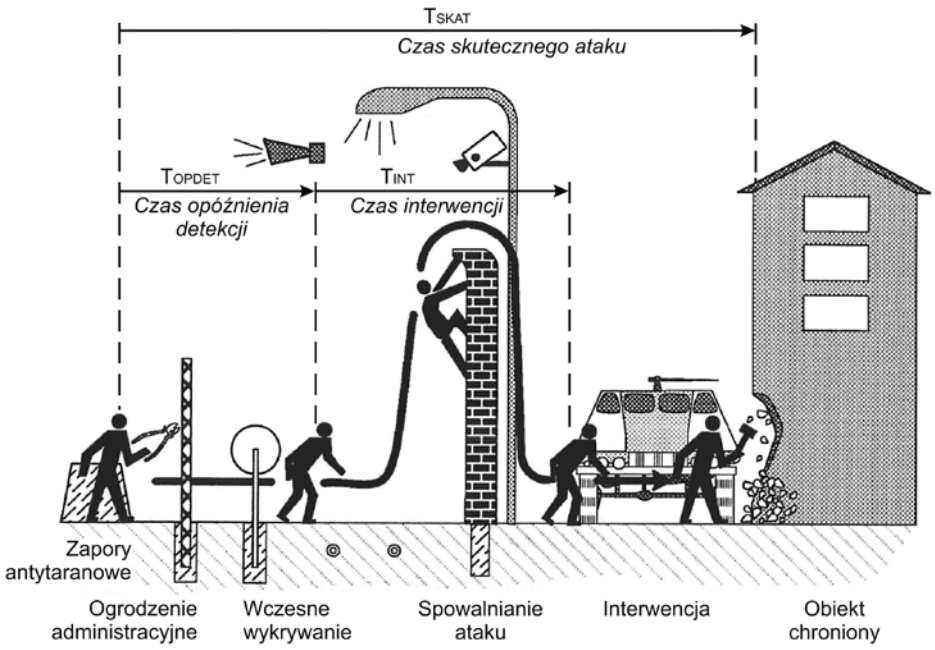
Przykładowy podział stref ochrony (od najbardziej chronionej):

1 – strefa ochrony wewnętrznej,
2 – strefa ochrony obrysowej,
3 – strefa ochrony peryferyjnej,
4 – strefa ochrony obwodowej (nazywana też z ang. strefą ochrony perymetrycznej),
5 – strefa dozoru zewnętrznego."

W poniższym artykule zostaną wyjaśnione pojęcia dotyczące stref ochrony zastosowane w NPOIK 2015.

Żeby zrozumieć zasady prawidłowego zabezpieczania, należy zdać sobie sprawę, że zagwarantowanie bezpieczeństwa nie obejdzie się bez umiejętnego powiązania zabezpieczeń elektronicznych i mechanicznych z interwencją fizyczną. Taką interwencję mogą realizować np. wewnętrzne służby ochrony lub podmioty zewnętrzne, wykonujące zadania ochrony osób i mienia w formie bezpośredniej ochrony fizycznej. Elektroniczny system sygnalizujący włamanie powinien jak najszybciej wykrywać naruszenie stref chro-

nionych, a system zabezpieczeń mechanicznych na tyle spowolnić działania intruzów, aby interweniujący mogli dotrzeć na czas. Okazuje się, że żaden z ww. systemów, działając w oderwaniu od innych, nie może zagwarantować skutecznego zabezpieczenia. Im wcześniej intruz zostanie wykryty, tym więcej czasu zostaje na przeprowadzenie skutecznej interwencji. System zabezpieczeń powinien być tak zaprojektowany, aby po wykryciu przez system alarmowy sygnalizacji włamania i napadu (SWiN) na intruzów czekały jeszcze przeszkody mechaniczne spowalniające ich działanie. Jeżeli system elektroniczny wykrywa naruszenie dopiero wewnątrz, gdy atakujący pokonali już zabezpieczenia mechaniczne, z reguły oznacza to, że system wykonano niezgodnie z przedstawioną zasadą prawidłowego zabezpieczania.



Rys. 1. Zależności czasowe w przypadku ataku na przykładowy obiekt infrastruktury krytycznej
Rys. Siemens

UMIEJĘTNOŚĆ POWIĄZANIA ZABEZPIECZEŃ ELEKTRONICZNYCH I MECHANICZNYCH Z INTERWENCJĄ FIZYCZNĄ

Zasada skutecznego zabezpieczania opiera się na walce z czasem. Prawidłowo zaprojektowany system daje szansę zapobieżenia popełnieniu przestępstwa, zaprojektowany nieprawidłowo co najwyżej poinformuje o jego popełnieniu. Z punktu widzenia zabezpieczenia infrastruktury krytycznej jest to szczególnie ważne. Błąd w założeniach ochrony IK może spowodować, że skutki dla bezpieczeństwa kraju mogą być katastrofalne. Podstawowym czynnikiem mającym wpływ na to, czy działania intruzów będą udane, jest czas trwania ataku – intuicyjnie wydaje się, że im dłużej będzie trwał, tym większe są szanse na jego udaremnienie. Żeby lepiej zrozumieć zasady zabezpieczania obiektów należących do infrastruktury krytycznej, należy zdefiniować przedziały czasów, które ułatwią taką analizę:

- **czas skutecznego ataku** (T_{SKAT}) – np. włamania, napadu czy ataku terrorystycznego – czas, po którym interwencja nie będzie miała znaczenia, ponieważ atak został zakończony sukcesem;
- **czas odporności mechanicznej** (T_{ODMECH}) – czas potrzebny intruzowi na przełamanie zabezpieczeń mechanicznych i dotarcia do celu swojego ataku. Traktujemy go jako czas zbiorczy, przyjmując zawsze zasadę „najsłabszego ogniwa";
- **czas opóźnienia detekcji** (T_{OPDET}) – czas liczony od momentu rozpoczęcia ataku, po upływie którego system alarmowy wyzwoli alarm i przekaże sygnał o alarmie do interweniujących;
- **czas interwencji** (T_{INT}) – czas od momentu wyzwolenia alarmu i powiadomienia o nim do rozpoczęcia skutecznej interwencji.

Na rys. 1. pokazano powyższe zależności czasowe odniesione do obiektu infrastruktury krytycznej. Należy zwrócić uwagę, że czas T_{SKAT} dla IK jest z reguły krótszy niż w analizach prowadzonych dla przestępstw pospolitych. Jeżeli zabezpieczamy np. przed kradzieżą, to czas T_{SKAT} kończy się w momencie, kiedy intruz opuści obszar chroniony, wynosząc skradzione przedmioty. W przypadku ochrony IK może się okazać, że T_{SKAT} kończy się w momencie dotarcia napastnika do celu swojego ataku (i na przykład zdetonowania przez niego ładunku wybuchowego). Przypatrzmy się poszczególnym elementom obrazującym zasady tworzenia ochrony przykładowego obiektu IK. Patrząc od lewej, dostęp jest chroniony przez bloki betonowe zabezpieczające przed siłowym wtargnięciem np. pojazdem. Mogą to być zapory antytaranowe, nazywane też zaporami antyterrorystycznymi, czy też zapory drogowe stałe lub ruchome. To ważny element, o którym często się zapomina – a trzeba mieć świadomość, że siłowe wtargnięcie pojazdu na chroniony teren degraduje precyzyjnie wymyślone plany ochrony, które nie uwzględniły takiej możliwości. Następnym ważnym elementem całej układanki jest ogrodzenie administracyjne wskazujące, gdzie zaczyna się obszar niedostępny dla osób postronnych. Ktoś, kto przekroczy ogrodzenie, nie może się potem tłumaczyć, że teren chroniony naruszył przez przypadek. Kolejnymi elementami są elektroniczne systemy wczesnego wykrywania intruzów (na rysunku zobrazowana została bariera mikrofalowa i kable detekcyjne zakopywane pod powierzchnią gruntu) oraz mur symbolizujący spowolnienie ataku. Transporter opancerzony to metafora interwencji fizycznej. Na podstawie analizy czasowej można wywnioskować, czy system ochrony IK został prawidłowo zaplanowany, zaprojektowany i wykonany.

Żeby uznać, że system zabezpieczeń został prawidłowo zaplanowany, zaprojektowany i wykonany, musi zostać spełniona poniższa zależność:

$$T_{ODMECH} > T_{OPDET} + T_{INT}$$

Jeżeli jest inaczej, to nie mamy do czynienia z systemem zabezpieczeń, a z systemem informującym o popełnieniu przestępstwa.

Rys. 2.1. Strefy ochrony sejfu bez wydzielonej strefy podejścia

Rys. 2.2. Strefy ochrony sejfu z wydzieloną strefą podejścia

STREFY OCHRONY

Aby dobrze zrozumieć podział obszarów należących do IK na strefy ochrony, należy ustalić, co jest obiektem chronionym i jaki jest cel ochrony.

Obiektem chronionym nazywamy przestrzeń ograniczoną barierą fizyczną, zwaną obrysem, wewnątrz której nie ma przeszkód uniemożliwiających intruzowi szybkie osiągnięcie celu swojego ataku. Jeżeli chronimy np. dokumenty w sejfie, obiektem chronionym jest sejf, a celem ochrony może być zabezpieczenie dokumentów przed kradzieżą. Gdy celem ochrony jest zabezpieczenie przed dostępem do komputera stojącego na biurku – wówczas obiektem chronionym jest pomieszczenie, w którym ten komputer się znajduje. Jeżeli intruz ma nieograniczony dostęp do infrastruktury krytycznej bezpośrednio po dostaniu się do budynku, wówczas obiektem chronionym jest budynek. Takie elastyczne podejście do zdefiniowania chronionego obiektu pozwoli na określenie ważnych obszarów związanych z jego zabezpieczeniem.

Na potrzeby taktyki ochrony **strefę wewnętrzną** (*internal zone*) obiektu chronionego zdefiniujemy jako przestrzeń, w której nie ma przeszkód uniemożliwiających intruzowi szybkie osiągnięcie celu ataku. Strefą wewnętrzną będzie wnętrze sejfu chroniącego dokumenty (jeśli jego wyniesienie z dokumentami jest mało prawdopodobne), obszar pomieszczenia, w którym na biurku stoi komputer, lub wnętrze budynku, gdy nieograniczony dostęp do witalnych elementów IK wiąże się z wtargnięciem intruza do budynku.

Obrysem obiektu chronionego będzie linia określająca granicę strefy wewnętrznej – w pierwszym przypadku: ściany i drzwi sejfu chroniącego dokumenty, w drugim przypadku: ściany, okna, drzwi, podłoga i sufit pomieszczenia, w którym znajduje się komputer, a w trzecim: graniczne ściany, okna, drzwi, podłogi i dach budynku, w którym intruz bezpośrednio po dostaniu się do środka ma nieograniczony dostęp do IK. Do strefy wewnętrznej przylega (na zewnątrz obrysu obiektu) **strefa peryferyjna** (*peripheral zone*). Obszar ochrony bezpośredniej kończy się na granicy strefy peryferyjnej, zwanej **obwodem** (*perimeter* – stąd ochronę obwodową nazywa się też ochroną perymetryczną), w rozumieniu zamkniętej linii otaczającej strefę peryferyjną. Poza strefą peryferyjną znajduje się **strefa zewnętrzna** (*external zone*), w której nie prowadzi się ochrony bezpośredniej (np. za ogrodzeniem chronionej instytucji). Takie zdefiniowanie stref jest dość ogólne i uniwersalne. W strefie peryferyjnej obiektów szczególnie zagrożonych, w obszarze przylegającym do obrysu (w najbliższej okolicy obiektu chronionego) wyznacza się czasami tzw. **strefę podejścia**. Przykładowo, jeżeli kilka obiektów chronionych ma wspólną strefą peryferyjną, wykrywanie w strefie podejścia może wskazywać, jaki jest cel ataku, dzięki czemu można lepiej zarządzać interwencją fizyczną. Na rys. 2.1, 2.2, 3.1, 3.2, 4.1 i 4.2 pokazano różnie zdefiniowane obiekty chronione (sejf, pomieszczenie i budynek) oraz dwie wersje podziału stref ochrony (ogólną i z wydzieloną strefą podejścia).

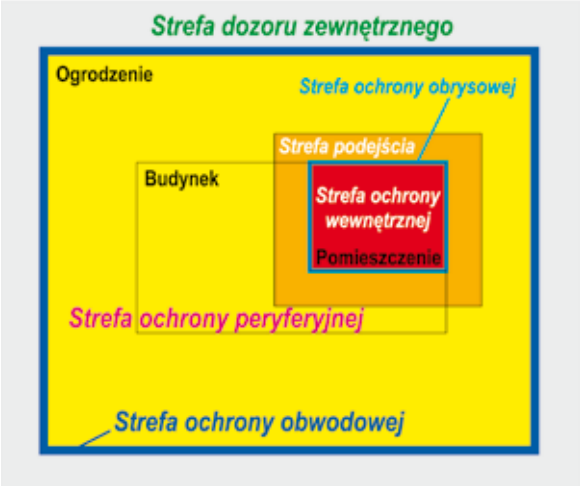
Rys. 3.1. Strefy ochrony pomieszczenia bez wydzielonej strefy podejścia

Na podstawie powyższych uzgodnień można dokonać podziału na strefy ochrony wymienione w Załączniku 1 do NPOIK 2015:

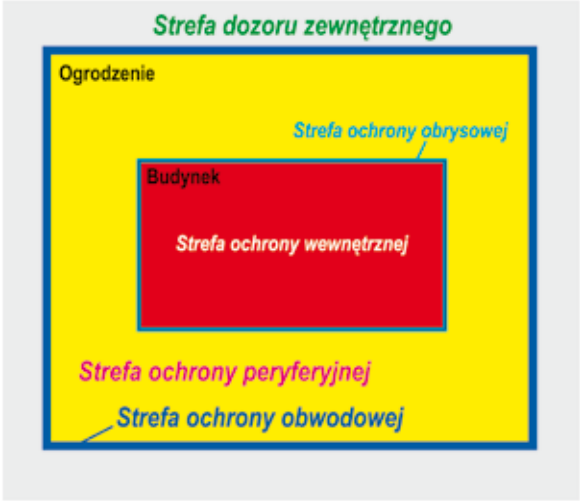
- **strefa ochrony wewnętrznej** – pamiętając, że jest to „ostatnia deska ratunku", bo będąc już w tej strefie, intruz nie ma przeszkód, aby szybko osiągnąć cel swojego ataku,
- **strefa ochrony obrysowej**,
- **strefa ochrony peryferyjnej** (czasem z wydzieloną strefą podejścia),
- **strefa ochrony obwodowej** (nazywanej też strefą ochrony perymetrycznej),
- **strefa dozoru zewnętrznego** (kontrolowana najczęściej przez system dozoru wizyjnego).

UWAGI KOŃCOWE

Nie od dziś wiadomo, że dziedzina projektowania i instalowania systemów zabezpieczeń jest w naszym kraju lekceważona. Wiele osób odpowiedzialnych za bezpieczeństwo IK, ale również projektujących zabezpieczenia, nie zostało prawidłowo przeszkolonych albo wręcz w ogóle nie przeszli szkoleń. Są zatem niewielkie szanse na to, iż IK w naszym kraju jest prawidłowo zabezpieczona. Branżowych projektantów i instalatorów „wyjętych spod prawa" budowlanego często „wyręczają" projektanci branży elektrycznej i wykonawcy instalacji elektrycznych. Ci, mimo że w prawie budowlanym są dobrze umocowani, z reguły nie mają podstawowej wiedzy o zasadach sztuki projektowania i instalowania systemów zabezpieczeń. Co gorsza, zwykle nawet nie zdają sobie z tego sprawy, a swoją „wiedzę" czerpią najczęściej z Internetu. A Internet jest wielkim, ale i nieuporządkowanym źródłem wiedzy. Żeby skorzystać z rzetelnych danych zamieszczonych w sieci, trzeba być fachowcem i umieć odróżnić informacje wartościowe od bezwartościowych, lub wręcz błędnych. Ponieważ wykonywanie zabezpieczeń wewnątrz budynków jest tanie i powszechnie stosowane, nagminnie rezygnuje się z organizowania najczęściej



Rys. 3.2. Strefy ochrony pomieszczenia z wydzieloną strefą podejścia



Rys. 4.1. Strefy ochrony budynku bez wydzielonej strefy podejścia

Rys. 4.2. Strefy ochrony budynku z wydzieloną strefą podejścia

niedających się niczym zastąpić stref ochrony: obrysowej, peryferyjnej czy obwodowej, które bardzo często wymuszają instalowanie urządzeń w warunkach zewnętrznych. A urządzenia pracujące w warunkach zewnętrznych są narażone na wiele zjawisk fizycznych, które mogą powodować alarmy niekoniecznie związane z pojawieniem się intruza. W związku z tym, jakość zastosowanych urządzeń, które sprawdzą się w warunkach zewnętrznych, przekłada się bezpośrednio na ich dość wysoką cenę, nie gwarantującą przy tym stuprocentowej odporności na pobudzenia zwodnicze (czyli wzbudzania fałszywych alarmów). Ale z tym należy się pogodzić, stawiając sobie za nadrzędny cel odpowiednie zabezpieczenie infrastruktury krytycznej.

Andrzej TOMCZAK
Ekspert PISA, pracownik dydaktyczny Ośrodka Szkoleniowego PISA, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym