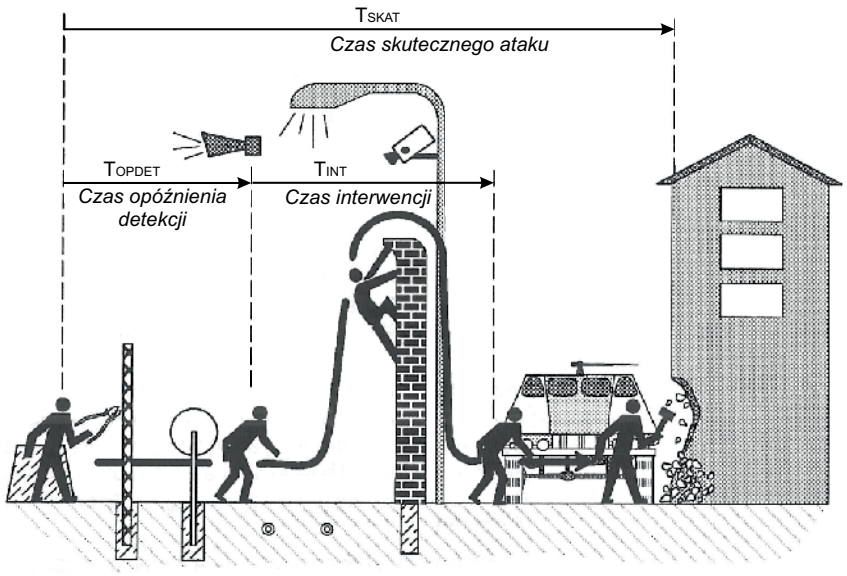
PODSTAWY ZABEZPIECZANIA
OBIEKTÓW INFRASTRUKTURY KRYTYCZNEJ

Andrzej Tomczak
ekspert PISA działający w KT 52 ds. systemów alarmowych przy PKN

Podstawową zasadą prawidłowego zabezpieczania obiektów jest umiejętne powiązanie zabezpieczeń elektronicznych i mechanicznych z interwencją fizyczną. Interwencję mogą realizować np. wewnętrzne służby ochrony czy prywatne agencje ochrony, wykonując zadania ochrony osób i mienia w formie bezpośredniej ochrony fizycznej.

Elektroniczny system sygnalizujący zagrożenie chronionych osób i mienia powinien jak najszybciej wykrywać intruzów, a system zabezpieczeń mechanicznych na tyle spowolnić ich działania, aby interweniujący dotarli na czas. Żaden z tych 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 na intruza – po wykryciu przez system alarmowy sygnalizacji włamania i napadu (SWiN) – czekały jeszcze przeszkody mechaniczne, spowalniające ich działanie. Jeżeli system elektroniczny wykrywa intruza dopiero wewnątrz, gdy ten pokonał już zabezpieczenia mechaniczne, tzn. 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

Skuteczne zabezpieczenia opierają się na odwiecznej 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 (IK) jest to szczególnie ważne. Drobna różnica w interpretacji, ale skutki dla bezpieczeństwa kraju mogą być diametralnie różne.

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 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 obiektów 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.

Przypatrzmy się poszczególnym elementom obrazującym zasady tworzenia ochrony przykładowego obiektu IK. Patrząc od lewej, dostępu do obiektu chronią bloki betonowe, zabezpieczające przed siłowym wtargnięciem np. pojazdem. Następnie jest ogrodzenie tzw. administracyjne, służące jako element wskazujący gdzie zaczyna się obszar niedostępny dla osób postronnych. Nikt, kto przekroczy ogrodzenie, nie może się potem tłumaczyć, że teren chroniony naruszył przez przypadek.

Kolejnymi elementami są elektroniczne systemy wczesnego wykrycia intruza (tutaj bariera mikrofalowa i kable detekcyjne zakopywane pod powierzchnią gruntu) oraz mur symbolizujący spowolnienie ataku intruza. Transporter opancerzony to metafora fizycznej interwencji. Na podstawie analizy czasowej można wywnioskować, w jakiej sytuacji system ochrony IK został zaprojektowany prawidłowo.

System zabezpieczeń został prawidłowo zaplanowany, zaprojektowany i wykonany, gdy:

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

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

STREFY OCHRONY W PRZYPADKU ZABEZPIECZANIA IK

Aby dobrze zrozumieć podział obiektów 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 kradzieżą notebooka leżącego na biurku – wówczas obiektem chronionym jest pomieszczenie, w którym ten notebook 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.

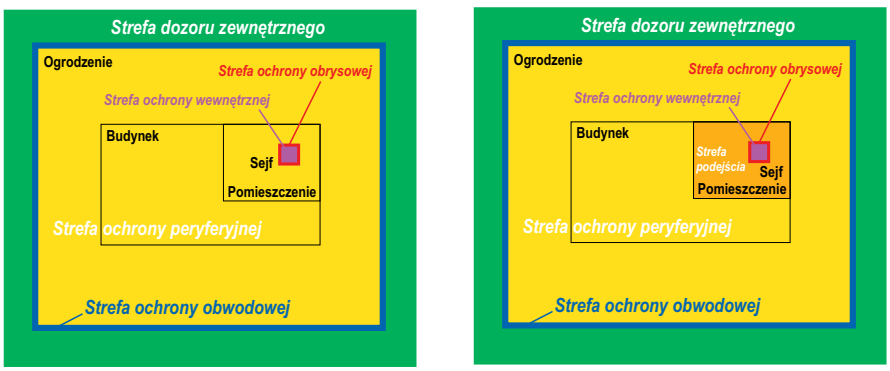
Na potrzeby taktyki ochrony **strefę wewnętrzną** *(internal zone)* obiektu chronionego zdefiniujemy jako przestrzeń, w której nie ma przeszkód uniemożliwiających intruzowi szybkie osiągnięcie celu ataku. Strefą wewnętrzną będzie wnętrze sejfu chroniącego dokumenty (jeśli jego wyniesienie z dokumentami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

Obrysem obiektu chronionego będzie linia określająca granicę strefy wewnętrznej – np. ściany i drzwi sejfu chroniącego dokumenty; ściany, okna, drzwi, podłoga i sufit pomieszczenia, w którym znajduje się notebook lub graniczne ściany, okna, drzwi, podłogi i dach budynku, w którym intruz, bezpośrednio po dostaniu się do środka, ma nieograniczony dostęp do IK.

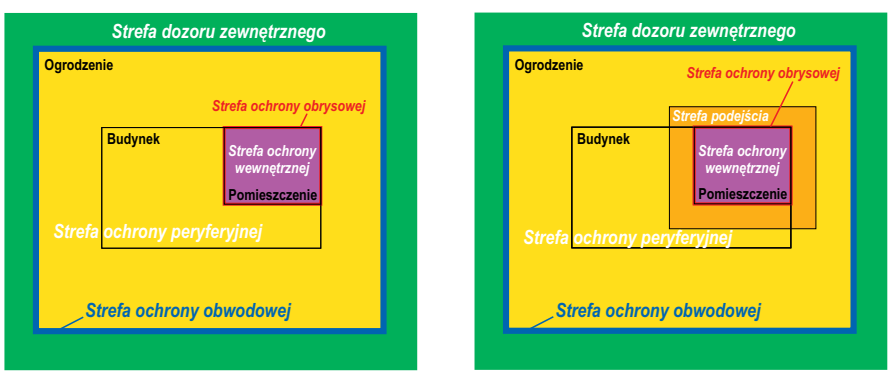
Do strefy wewnętrznej przylega (na zewnątrz obrysu obiektu) **strefa peryferyjna** *(peripheral zone)*. Obszar ochrony bezpośredniej kończy się na granicy strefy peryferyjnej, zwanej **obwodem** *(perimeter* – stąd ochronę obwodową nazywa się też ochroną perymetryczną), w rozumieniu zamkniętej linii otaczającej strefę peryferyjną. Poza strefą peryferyjną znajduje się **strefa zewnętrz-**

na *(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, to wykrywanie w strefie podejścia może wskazywać, jaki jest cel ataku, dzięki czemu można lepiej zarządzać interwencją fizyczną. Na rys. 2, 3 i 4 pokazano różnie zdefiniowane obiekty chronione (sejf, pomieszczenie i budynek) oraz dwie wersje podziału stref ochrony (ogólną i z wydzieloną strefą podejścia).

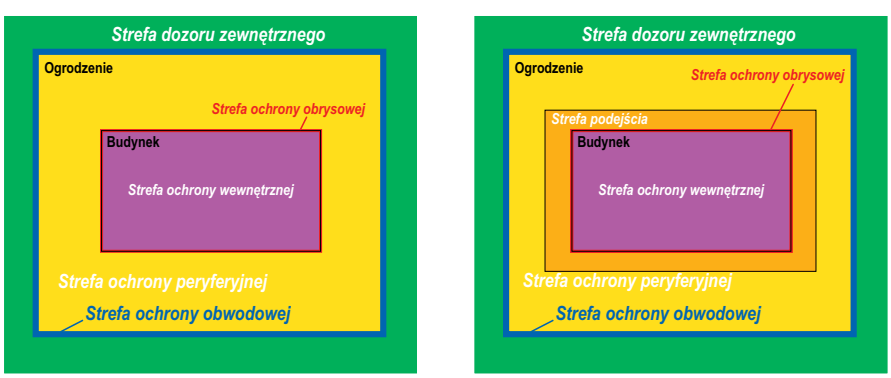
Rys. 2. Strefy ochrony sejfu bez wydzielonej i z wydzieloną strefą podejścia



Rys. 3. Strefy ochrony pomieszczenia bez wydzielonej i z wydzieloną strefą podejścia



Rys. 4. Strefy ochrony budynku bez wydzielonej i z wydzieloną strefą podejścia



Reasumując, można dokonać podziału na następujące strefy ochrony:

- **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

Dlaczego tak wiele instalowanych systemów zabezpieczeń IK wykonywanych jest niezgodnie z omówionymi zasadami?
Nie od dziś wiadomo, że dziedzina projektowania i instalowania systemów zabezpieczeń jest w Polsce traktowana po macoszemu. Wiele osób odpowiedzialnych za zabezpieczenie obiektów, ale również projektujących zabezpieczenia, nie zostało prawidłowo przeszkolonych (albo w ogóle nie przeszli szkoleń), popełniają więc nawet podstawowe błędy.
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 zabezpieczeń elektronicznych. 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). Nie należy kierować się wyłącznie popularnością wejść na poszczególne strony WWW!
Wykonywanie zabezpieczeń wewnątrz obiektów jest prostsze i tańsze niż zrealizowanie ochrony: obrysowej, peryferyjnej czy obwodowej, która bardzo często wymusza 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 urządzeń przekłada się bezpośrednio na ich dość wysoką cenę, nie gwarantując przy tym 100% odporności na pobudzenia zwodnicze (czyli wzbudzania tzw. fałszywych alarmów). Ale z tym należy się pogodzić, stawiając sobie za nadrzędny cel odpowiednie zabezpieczenie infrastruktury krytycznej.