

Załącznik nr 8 – Organizacja systemu sygnalizacji włamania i napadu (SSWiN).

Określone w Załączniku rozwiązania organizacyjne i techniczne stosowane są zgodnie z opracowaną przez Pion Bezpieczeństwa kategoryzacją typów obiektów, o której mowa w Rozdziale I pkt 5 Regulaminu określającego standardy bezpieczeństwa fizycznego.

Wymagania formalne

Normy

- PN-EN 50131 Systemy alarmowe - Systemy sygnalizacji włamania i napadu, Wymagania systemowe.

Zasady ogólne

Obiekty technologiczne Spółki, m.in. tłocznie, węzły, osuszalnie lub stacje gazowe, mogą być narażone na zagrożenia zewnętrzne i wewnętrzne. Ewentualne zniszczenia infrastruktury gazowej mogą skutkować bardzo dużymi stratami materialnymi oraz stanowić zagrożenie dla życia i zdrowia ludzi. Analiza możliwych zagrożeń klasyfikuje te obiekty do kategorii stopnia zabezpieczenia 3 (ryzyko średnie), a w dużej części do stopnia zabezpieczenia 4 (ryzyko wysokie) wg. normy **PN-EN 50131**, część 7 – Wytyczne stosowania. Wykonywane systemy powinny spełniać wymagania zalecane dla 3 stopnia zabezpieczenia zgodnie z normą **PN-EN 50131**.

System SWiN powinien być wykonywany jako dwustrefowy:

- strefa ochrony obwodowej,
- strefa ochrony wewnętrznej (wybrane pomieszczenia w budynkach technologicznych).

System ochrony obwodowej powinien objąć ochroną zewnętrzną najdalej wysuniętą część obiektu obejmującą najczęściej ogrodzenie lub jego otoczenie. Zalecanym rozwiązaniem jest montaż czujników alarmowych bezpośrednio na ogrodzeniu obiektu, bramie i furtce.

Wymagania funkcjonalne systemu:

- duża skuteczność wykrywania prób sforsowania ogrodzenia (przechodzenia, podnoszenia, przecinania),
- dokładna lokalizacja miejsca forsowania,
- niski współczynnik fałszywych alarmów, wywoływanych przez wiatr oraz opady atmosferyczne,
- niezależna konfiguracja detektorów, umożliwiająca dostosowanie parametrów czujników do jakości ogrodzenia.

Alternatywnym rozwiązaniem, wynikającym z uwarunkowań danego obiektu (np. architektonicznych), może być zastosowanie przestrzennych czujników ruchu, których ilość i lokalizacja powinna zapewnić ochronę całego wewnętrznego pasa przyogrodzeniowego. Przestrzenne czujniki ruchu powinny zapewniać skuteczne wykrycie intruza w polu działania, przy uwzględnieniu niskiego współczynnika fałszywych alarmów.

Wszystkie urządzenia zewnętrzne powinny posiadać III lub IV klasę środowiskową zgodnie z normą **PN-EN 50131**.

System ochrony wewnętrznej powinien objąć ochroną wybrane pomieszczenia w budynkach technologicznych (pomieszczenia AKP, sterownie, rozdzielnie elektryczne itp.).

System powinien być wyposażony w dedykowany moduł komunikacji ETHM do realizacji połączenia z nadrzędnym stanowiskiem obsługi użytkownika lub inny tor transmisji danych, umożliwiający nadzór i obsługę systemów z jednego stanowiska (w obrębie poszczególnych Oddziałów). Lokalna obsługa systemu powinna być realizowana z poziomu manipulatora sztyrowego. Wybrane lokalizacje należy wyposażyć w tablicę synoptyczną.

System SWiN powinien być wykonany jako niezależny od innych systemów (SKD, CCTV), a ewentualna integracja z innymi systemami nie może wpływać na samodzielne i niezależne funkcjonowanie systemu.

W przypadku obiektów nieposiadających stałej ochrony fizycznej; stany alarmowe oraz wybrane informacje techniczne powinny być przestane do zewnętrznych służb ochrony (Grupa Interwencyjnych) oraz włączone do sterowników PLC stanowiących źródło danych dla systemu SCADA. Komunikacja z PLC musi odbywać się za pośrednictwem sygnałów binarnych, dostosowanych elektrycznie do rodzaju wejść binarnych sterownika. Inny sposób nie jest dopuszczalny. Lokalna sygnalizacja alarmu powinna być realizowana poprzez sygnalizatory optyczno-akustyczne. Uzbrowanie i rozbrojenie stref alarmowych powinno być realizowane przy użyciu kart kontroli dostępu.

Rozbrojenie i uzbrowienie strefy alarmowej obiektu powinno być sygnalizowane optycznie lub/i akustycznie (jednoznaczna interpretacja stanu systemu dla użytkownika dokonującego tej czynności). Użytkownik dokonujący rozbrojenia lub uzbrowienia systemu alarmowego zobowiązany jest powiadomić i dokonać autoryzacji wykonanej czynności z nadzorem systemu (lokalną ODG lub wskazaną komórką Pionu Bezpieczeństwa).

Rozwiązania organizacyjne

Administratorem systemów SWiN jest Pion Bezpieczeństwa. Wszystkie urządzenia SSWiN muszą zostać podłączone do wydzielonej fizycznie sieci LAN lub do segmentu sieci SKD (V-LAN). Parametry segmentu sieci określone zostały w załączniku nr 6 - **Organizacja systemu kontroli dostępu (SKD) – Rozwiązania organizacyjne.**

Pion Bezpieczeństwa

Zastępca Dyrektora



Tomasz Kucharski