

Załącznik nr 6 – Organizacja systemu kontroli dostępu (SKD).

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 60839 Systemy alarmowe i elektroniczne systemy zabezpieczeń.

Zasady ogólne

Przy projektowaniu i instalowaniu SKD, należy kierować się przede wszystkim obowiązującymi standardami, funkcjonalnością i normą **PN-EN 60839**. Do zabezpieczenia obiektów należy wykonywać systemy w 3 stopniu zabezpieczenia. Należy mieć na uwadze, że w normie dotyczącej SKD, nie określa się stopnia zabezpieczenia dla całego systemu, lecz przypisuje się stopnie zabezpieczenia poszczególnym funkcjonalnościom, określanym indywidualnie dla każdego przejścia kontrolowanego. Pozwala to na stosowanie w tej samej instalacji urządzeń o niższym stopniu zabezpieczenia. Dopuszcza się zastosowanie czytnika dostępu 1 stopnia do kontrolera lub centrali 4 stopnia, lecz nie odwrotnie. Stopień zabezpieczenia powinien być wyższy analogicznie do struktury funkcjonalnej systemu dla urządzeń głównych.

Jednym z ważniejszych wymagań, jest funkcjonalność systemu, polegająca na jego odporności na próbę sabotażu oraz ingerencji, celem zakłócenia działania lub skopiowania kart dostępu. Dla systemu SKD, należy przyjąć minimalny czas pracy na zasilaniu rezerwowym, wynoszący minimum 4 h dla wszystkich elementów, łącznie z urządzeniami blokującymi oraz monitorującymi przejścia. Wymóg 4h pracy na zasilaniu rezerwowym, o ile nie ma specjalnych wytycznych, nie dotyczy urządzeń o znacznym poborze mocy np. szlabany, bramy uchylne i przesuwne, słupki antyterrorystyczne. Informacja o braku zasilania sieciowego 230V systemu SKD z obiektów bezobsługowych musi być wysłana do odpowiednich służb nadzoru zewnętrznego.

Każda instalacja SKD na obiektach o stałej ochronie fizycznej, powinna być wyposażona obligatoryjnie w wizualizację stanów przejść na monitorze podglądowym, zlokalizowanym na posterunku ochrony. Do blokowania drzwi należy stosować tylko zwory elektromagnetyczne połączone z przyciskami ewakuacji. Wciśnięcie przycisku ewakuacji powinno wygenerować alarm siłowego otwarcia drzwi. Ponadto stan zbyt długiego czasu otwarcia drzwi, powinien zostać zasygnalizowany stanem alarmowym. Główne urządzenia systemu SKD należy lokalizować w pomieszczeniach zabezpieczonych przed dostępem osób nieuprawnionych i zabezpieczonych systemem SSWiN oraz SKD.

Obszary i miejsca, które w szczególności należy objąć systemem kontroli dostępu:

- bramy i szlabany wjazdowe oraz przejazdowe na terenie obiektu,
- bramki, furtki, kołowrotki na terenie obiektu,
- drzwi wejściowe do budynków administracyjnych,
- serwerownie,

- archiwa zakładowe,
- Dyspozycje Gazu, w tym zapasowe,
- punkty dystrybucji sieci informatycznej,
- pomieszczenia Pionu Bezpieczeństwa,
- pomieszczenia Zarządu Spółki, wytypowane pomieszczenia kierowników jednostek organizacyjnych, Kancelaria Tajna, itp.

Dodatkowe funkcjonalności dla Systemu Kontroli Dostępu:


- praca wielostanowiskowa,
- komunikacja kontrolerów z czytnikami i ekspanderami szyfrowana,
- obsługa kart MIFARE DESFire EV1,
- zarządzanie i konfigurowanie przez wielu operatorów,
- raportowanie czasu obecności,
- integracja z systemem alarmowym,
- integracja z systemem CCTV,
- kontrola dostępu w windach konwencjonalnych,
- kontrola dostępu do depozytorów i szafek,
- awaryjne otwieranie i zamykanie przejść,
- rejestracja na bieżąco wszystkich zdarzeń w systemie,
- możliwość automatycznego powiadamiania o wystąpieniu dowolnego zdarzenia drogą email, wyświetleniu na ekranie monitora, wystaniu pakietu danych (protokołem TCP) pod wskazany adres sieciowy,
- kontrola liczby osób w strefie (łącznie z ustaleniem ich limitu),
- funkcja Anti-passback, weryfikacja otwarcia drzwi, przejścia typu śluza, przejścia dwustronne z rozróżnieniem kierunku przejścia,
- harmonogramy uzależniające działanie systemu od dni i godzin,
- możliwość tworzenia grup użytkowników, stref dostępu, stref obwodowych,
- przesyłanie ustawień do kontrolerów bez zatrzymywania pracy systemu.

Rozwiązania organizacyjne

Administratorem systemu kontroli dostępu jest Pion Bezpieczeństwa. Wszystkie urządzenia SKD muszą zostać podłączone połączeniem kablowym do wydzielonej fizycznie sieci LAN lub do segmentu sieci SKD (V-LAN).

Parametry segmentu sieci dla systemów SKD:

1. Segment obejmuje daną lokalizację fizyczną z uwzględnieniem wszystkich niezbędnych do działania systemów KD i SSWIN elementów technicznych i technologicznych, w tym urządzenia Elektronicznego Systemu Zarządzania Kluczami (depozytory);
2. W obrębie jednego wybranego segmentu muszą zostać umieszczone komputery do wykonywania czynności administratorskich (stacje inżynierskie);
3. Stacje inżynierskie muszą komunikować się z elementami technicznymi i technologicznymi systemów KD ze wszystkich segmentów Spółki;
4. Segment może komunikować się z siecią LAN\WAN jedynie w zakresie niezbędnych portów TCP do utrzymania następujących usług:
 - a. Usługa katalogowa Active Directory,
 - b. Serwer czasu,
 - c. Serwer pocztowy,
 - d. Serwer wydruku,
 - e. Serwer ochrony antywirusowej funkcjonującego w Spółce,
 - f. Serwer zdalnych aktualizacji systemów operacyjnych WSUS,
 - g. Serwer zdalnych aktualizacji i konfiguracji oprogramowania SCCM
 - h. Serwery aktywacyjne - KMS
 - i. Serwer zarządzania zgodnością licencyjną SAM
 - j. Serwer zarządzania szyfrowaniem dysków twardych.
 - k. Serwer komunikacji Roger.
 - l. Dostęp zdalny do stacji inżynierskich ze ściśle określonych stacji dla uprawnionych użytkowników Pionu Bezpieczeństwa bez możliwości podłączania zasobów lokalnych i zdalnych,
 - m. Dostęp do udostępnionego zasobu na stacji inżynierskiej ze ściśle określonych stacji Pionu Bezpieczeństwa dla uprawnionych użytkowników,
5. Pracownicy Pionu Bezpieczeństwa do pracy na stacjach inżynierskich będą wykorzystywać oddzielne konta o podwyższonych uprawnieniach (zaakceptowane odstępstwo od zasad bezpieczeństwa).

Pion Bezpieczeństwa
Zastępca Dyrektora

Tomasz Kucharski

