

**WYTYCZNE
DO PROJEKTOWANIA INSTALACJI TELETECHNICZNYCH
I TELEINFORMATYCZNYCH W NOWYM OBIEKCIE ZARZĄDU
CENTRALNEGO BIURA ZWALCZANIA CYBERPRZESTĘPCZOŚCI
w Gdańsku przy ul. Harfowej 60**

1. Pomieszczenia.

1.1. Serwerownia.

Pomieszczenie urządzeń teletransmisyjnych, Głównego Punktu Dystrybucyjnego (GPD) okablowania strukturalnego budynku oraz głównych urządzeń instalacji dozoru obiektu.

- wymaga się wykonania pomieszczenia serwerowni o powierzchni ok. 70m² (4,8m x 14,6m) z dwuskrzydłowymi drzwiami pożarowymi EI60 o wymiarach 150cm x 220cm.
- w pomieszczeniu tym umieszczone zostaną szafy Rack w ilości do 12 szt. o wymiarach max. 45U 800x1000mm/szer x gł/ ,
- system klimatyzacji precyzyjnej N+1 (obciążenie pojedynczej szafy należy przyjąć na poziomie 6kW),
- szafy w jednym rzędzie, bokami do siebie, z dostępem z przodu i z tyłu stojaków, drzwi do szaf ażurowe. Szafy Rack wyposażać między innymi w panele wentylacyjne, panele dystrybucji napięć, listwy zasilające 8-gniazdowe z wyłącznikiem i układem pomiarowym natężenia prądu umożliwiający jego odczyt, panele porządkujące poziome i pionowe, po 3 półki na urządzenia.
- w pomieszczeniu stanowiska dla czterech komputerów systemowych i 2 osób, operatorów systemów,
- wymagana wysokość pomieszczenia to 3,5 m,
- serwerownia musi być wyposażona w podłogę techniczną (60cm),
- kanały kablowe montować w części podsufitowej.

1.2. Dodatkowe wymagania.

- klimatyzacja powinna zapewnić stałą temperaturę 20-22°C;
- pom. serwerowni najlepiej projektować w centralnej części budynku, na piętrze
- okna przesłonięte markizą zewnętrzną nie przepuszczającą promieni słonecznych;
- ściany murowane, drzwi wzmacniane;
- wszystkie ściany, posadzkę oraz strop, w przypadku wykończenia wyprawami tynkarskimi po zagruntowaniu należy pomalować farbą lateksową w kolorze białym. Dopuszcza się inne rozwiązania pod warunkiem zapewnienia odpowiedniego zabezpieczenia przed pyleniem;
- podłoga – antyelektrostatyczna;

- oświetlenie jak dla biur projektowych;
- uziemienie, o wartości nie większej niż 1,5 ohm, doprowadzone na listwę zaciskową.

1.3. Szachty instalacyjne.

Dla potrzeb serwerowni należy zaprojektować wydzielone szachty dla:

- obsługi klimatyzacji i wentylacji,
- instalacji elektrycznych ,
- okablowania strukturalnego,
- do serwerowni należy doprowadzić wodę do nawilżaczy AC i zaprojektować kanalizację dla skroplin.

2. Infrastruktura telekomunikacyjna zewnątrzna.

2.1. Kanalizacja teletechniczna.

Na potrzeby niniejszego budynku przyjęto następujące wstępne założenia dot. kanalizacji teletechnicznej :

- wybudować dwa niezależne ciągi dwuotworowej kanalizacji teletechnicznej pomiędzy istniejącą serwerownią OPP a pomieszczeniem serwerowni CBZC wykorzystując istniejące ciągi kanalizacji na terenie OPP,
- wybudować odcinek kanalizacji teletechnicznej dwuotworowej od serwerowni CBZC do studni operatora przy głównej bramie wjazdowej od strony ul. Harfowej,
- kanalizację wprowadzić do obiektu CBZC poprzez studnie telekomunikacyjne pod budynkowe SKR-2 i doprowadzić do pom serwerowni (GPD). W studniach pod budynkowych SKR-2 zaprojektować stelaże zapasu dla wprowadzanych do budynku kabli.

Szczegółowy zakres robót instalacyjnych w terenie winien być określony na etapie opracowania dokumentacji projektowej, z uwzględnieniem warunków technicznych przyłączenia do sieci operatora telekomunikacyjnego.

2.2. Sieć kablowa na terenie obiektu.

Wybudować dwa kable światłowodowe OTK 24J dwoma niezależnymi ciągami kanalizacji teletechnicznej pomiędzy serwerownią OPP a serwerownią CBZC. Kable zakończyć na przełącznicami optycznymi po obu końcach złączami E2000/APC. W serwerowni OPP przełącznicę światłowodową zainstalować w istniejącej szafie dedykowanej do kabli światłowodowych, a w serwerowni CBZC w projektowanej szafie dedykowanej do urządzeń transmisyjnych. Ponadto należy wybudować kabel telekomunikacyjny XzTKMxpw 10x4x0,6 krótszą trasą kanalizacji pomiędzy serwerowniami OPP i CBZC. Kabel wieloparowy w serwerowni CBZC zakończyć w tej samej szafie co kabel światłowodowy i zaterminować go na patchpanelu RJ45 lub łączówkami KRONE LSA+ (rozłącznymi). W pomieszczeniu serwerowni

istniejącego budynku OPP zakończyć łączówkami KRONE LSA+ (rozłącznymi) na PG łączówkami KRONE LSA+ (rozłącznymi).

3. Systemy teleinformatyczne.

3.1. System okablowania strukturalnego:

W budynku zaprojektować okablowanie strukturalne sieci LAN w oparciu o aktualne normy ISO/IEC11801 (wersja ostateczna), EIA/TIA 568 B (wersja ostateczna) oraz EN 50173-2. Budowę okablowania zaleca się opierać o kable UTP 4x2x0,5 LSOH kategorii min. 6a oraz o kable światłowodowe – jednomodowe.

Okablowanie strukturalne powinno integrować wszystkie systemy teletechniczne włącznie z siecią telefonii VoIP.

W zakres opracowania wchodzi:

- instalacja okablowania poziomego,
- instalacja okablowania pionowego,
- zainstalowanie punktu dystrybucyjnego,
- wykonanie punktów przyłączeniowych RJ45 na potrzeby sieci komputerowej.

Instalację zakończyć gniazdami typu RJ-45 z jednej strony w punkcie dystrybucyjnym GPD, w szafach dystrybucyjnych 19" (dobrać odpowiednio do pojemności sieci), a z drugiej strony w punktach przyłączeniowych elektryczno-logicznych PEL na stanowiskach pracy.

Punkty elektryczno-logiczne PEL składają się z 4 gniazd RJ-45 umożliwiających podłączenie komputera i/lub telefonu, dwóch gniazd światłowodowych oraz dwóch podwójnych gniazd elektrycznych, z blokadą, zasilanych z UPS centralnego poprzez dedykowaną sieć zasilania komputerów. Szczegółowy opis 3 rodzajów PEL przedstawiono w pkt. 3.1.2.

Główny Punkt Dystrybucyjny zostanie wykonany w pomieszczeniu serwerowni na parterze budynku, przeznaczonym na potrzeby urządzeń łączności i informatyki, w postaci min. 2 szaf dystrybucyjnych z panelami krosowniczymi kat. 6a, z gniazdami RJ-45 oraz dwoma listwami zasilającymi po min. 8 gniazd każda, z sygnalizacją optyczną napięcia i wyłącznikiem listwy. Ponadto listwy zasilające powinny być wyposażone w układy pomiarowe umożliwiające odczyt zużywanego prądu. Wszystkie szafy w serwerowni zasilic z dwóch źródeł : UPS'a oraz siłowni telekomunikacyjnej (oddzielne listwy zasilające). Każdą listwę zasilającą należy zasilic z oddzielnego obwodu elektrycznego zabezpieczonego wyłącznikiem nadprądowym w rozdzielni.

Światłowody zakończyć na panelu krosowym z gniazdami typu SC/APC.

Elementy pasywne sieci strukturalnej powinny posiadać świadectwa co najmniej jednego niezależnego laboratorium badawczego.

Wszystkie komponenty systemu okablowania będą posiadały parametry w kategorii 6a – channel.

Wszystkie komponenty systemu okablowania strukturalnego część logiczna, będą wyprodukowane przez jednego producenta, poświadczone certyfikatem.

Całość oferowanej instalacji okablowania strukturalnego dla wskazanych lokalizacji musi posiadać możliwość dalszej rozbudowy w części logicznej: posiadać przekroje tras kablowych oraz wielkość szafy dystrybucyjnej dostosowane do zwiększenia struktury o 25%.

Główne piony kablowe prowadzić w wydzielonych dla teleinformatyki szachtach kablowych p/t, z drzwiczkami rewizyjnymi na piętrach.

Gwarancja producenta na okablowanie powinna wynosić min. 20 lat.

Łącze należy traktować jako pełen tor transmisyjny składający się z kabla, patch-cordów, patch-paneli oraz gniazd przyłączeniowych.

System okablowania w szafie dystrybucyjnej ma się składać z 24 lub 48 portowych paneli, z gniazdami RJ45, wytrzymałych na co najmniej 750-krotne operacje włączenia i wyłączenia kabli połączeniowych i krosujących. System okablowania strukturalnego musi być wyposażony w funkcje zarządzania okablowaniem bez konieczności stosowania niestandardowych kabli krosowniczych.

Okablowania poziome

Długość przewodu od punktu dystrybucyjnego do gniazda nie może przekraczać 90 m.

Na potrzeby okablowania strukturalnego należy ułożyć koryta kablowe. Na korytarzach przewody prowadzić w przestrzeni międzystropowej, natomiast w pomieszczeniach przewody należy wciągać do peszli i układać w konstrukcji ścian działowych.

3.1.1. Okablowanie strukturalne dla sieci niejawnych.

W budynku przewidzieć wydzieloną sieć okablowania strukturalnego dla potrzeb sieci niejawnych. Pomieszczenia do których należy doprowadzić sieć niejawną zostaną określone przez użytkownika. Kable oraz osprzęt projektować w innym kolorze niż sieć główna. Dla sieci niejawnej zaprojektować w serwerowni dedykowaną szafę rack i w niej zakończyć okablowanie w technologii jak dla całego obiektu.

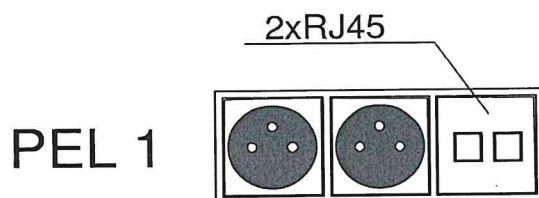
Na potrzeby sieci niejawnej należy wykonać punkt przyłączeniowy złożony z zestawu gniazd PEL1 (pkt. 3.1.2).

3.1.2. Punkt elektryczno - logiczny.

W obiekcie przewidziano 3 rodzaje zestawów gniazd PEL - punktów elektryczno-logicznych:

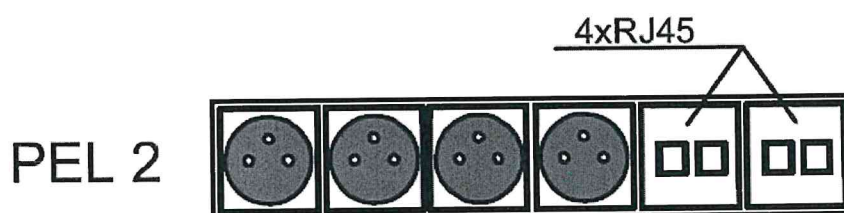
PEL1

Zespół gniazd złożonych z 2 gniazd RJ45 kat. 6a oraz 2 gniazd zasilania 2P+0 (zasilane podtrzymania UPS) umieszczone w jednym zespole gniazd natynkowych lub podtynkowych.



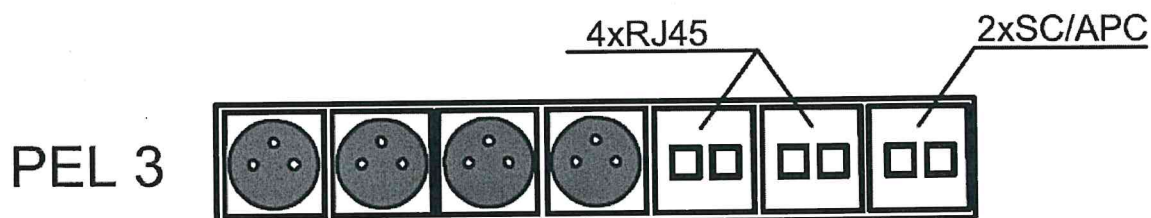
PEL2

Zespół gniazd złożonych z 4 gniazd RJ45 kat. 6a oraz 4 gniazd zasilania 2P+0 z blokadą (tzw. gniazda DATA) umieszczone w jednym zespole gniazd natynkowych lub podtynkowych.



PEL3

Zespół gniazd złożonych z 4 gniazd RJ45 kat. 6a i 2 gniazd światłowodowych (2xSC/APC) oraz 4 gniazd zasilania 2P+0 z blokadą (tzw. gniazda DATA) umieszczone w jednym zespole gniazd natynkowych lub podtynkowych.



Na potrzeby podłączenia drukarek sieciowych/urządzeń wielofunkcyjnych należy wykonać punkt przyłączeniowy złożony z zestawu gniazd PEL1.

W każdym pokoju 1 osobowym przewiduje się na każde stanowisko pracy komputerowej zestaw gniazd PEL2 i PEL3 oraz po punkcie rezerwowym PEL2 i PEL3 umieszczonym w pozostałej części pomieszczenia.

W pozostałych pomieszczeniach biurowych przewiduje się, iż na każde stanowisko pracy komputerowej przewiduje się zestaw gniazd PEL2 i PEL3.

Zestaw gniazd PEL 2 projektować w pom. RG i UPS oraz pom. socjalnych, magazynach itp.

W pomieszczeniach specjalnych oraz salach odpraw, zamontować florboxy.

Uwzględnić, przy ciągach komunikacyjnych, dedykowane miejsca (w postaci wnęk) na każdej z kondygnacji dla urządzeń wielofunkcyjnych (szer./głęb. 130/90 cm) oraz przewidzieć dla nich podłączenie zarówno do sieci elektrycznej jak i sieci logicznej (strukturalnej).

Ilość miejsc przygotowanych do instalacji urządzeń wielofunkcyjnych należy ustalić z Inwestorem lecz nie mniej niż 2 miejsca na każdej kondygnacji.

Na korytarzach należy umieścić gniazda 1xRJ45 na potrzeby podłączenia punktów rozsiewczych Acces Point. Punkty przyłączeniowe powinny być tak zlokalizowane, aby zasięg radiowy obejmował wszystkie pomieszczenia w budynku (za wyjątkiem pom. ekranowanych).

Wymagania dot. dokumentacji powykonawcza sieci strukturalnej

Dokumentacja powinna zawierać m.in. komplet informacji o rozmieszczeniu gniazd, relacji wszystkich kabli i trasach prowadzenia wszystkich wykonanych torów kablowych na obiekcie. Dołączyć należy także raporty z wykonanych pomiarów oraz karty katalogowe, aprobaty, certyfikaty wszystkich elementów użytych przy budowie instalacji teletechnicznej.

Pomiarów wszystkich wykonanych instalacji należy dokonać z wykorzystaniem certyfikowanych mierników pomiarowych, umożliwiających wygenerowanie graficznych raportów, posiadających aktualną kalibrację potwierdzoną przez producenta miernika. Pomiary muszą być wykonane zgodnie z obowiązującymi polskimi normami, a wyniki pomiarów powinny odpowiadać podanym w tych normach wartościom.

Dokumentację należy wykonać zarówno w formie papierowej jak i elektronicznej dostarczonej na załączanym nośniku. Do wersji elektronicznej dokumentacji należy dołączyć wszelkie schematy i opisy dotyczące opracowania w postaci edytowalnej (doc/dwg). Wymaga się załączenia plików z urządzenia pomiarowego w postaci oryginalnej.

3.2. Urządzenia aktywne w serwerowni

Zaprojektować urządzenia aktywne w postaci switchy:

- Switche Cisco Catalyst 9200L 48-portów 10/100/1000 (PoE+), 4 porty 10 Gigabit SFP+,
- Switche Cisco C9500- 48X-E, SFP+ SFP-10G-SR
- Router ASR 1001-x,
- Dwa niezależne zestawy w ukompletowaniu dwa fizyczne serwery (pod serwery wirtualne) i macierz dyskowa (min 100TB) z licencjami,
- Oprogramowanie Goverlan, MS Active Directory, bezpieczny wydruk podążający, VMware,

3.3. Sieć WiFi

Zaprojektować sieć bezprzewodową WiFi dla wszystkich pomieszczeń obiektu w oparciu o międzynarodowe normy IEEE 802.11i. dla 2,4Ghz i 5,2GHz. Rozwiązanie musi zapewniać dostęp wyłącznie uprawnionym podmiotom oraz zapewnić poufność transmisji danych.

3.4. System telefoniczny VoIP i urządzenia współpracujące.

Należy przewidzieć włączenie obiektu w system telefonii IP KGP opartego o Cisco Call managera 12.5.1.11900-146. System telefonii VoIP będzie obsługiwać wszystkie wydziały zlokalizowane w obiekcie. Stanowiska kierownicze należy wyposażyć w terminale telefoniczne Cisco CP-8865 z przystawką oraz w 5 szt. bezprzewodowych słuchawek CP-8821, pozostałe stanowiska wyposażyć w terminale Cisco CP-7821. W projekcie ująć zakup licencji do wszystkich telefonów. Poprzez węzeł VoIP dostępna będzie sieć operatora publicznego oraz sieć resortowa policji.

3.5. System monitoringu obiektu CCTV.

W budynku planuje się wykonanie instalacji telewizji dozorowej CCTV.

Systemem telewizji dozorowej obiektu CCTV objąć korytarze, wejścia do budynku, do archiwów, serwerowni, do stref zamkniętych, pomieszczeń specjalnych /np. magazyny broni/, teren wokół budynku jak również teren przyległy do budynku /wjazdy, parkingi, budynki techniczne/. System powinien wykorzystywać instalacje w standardzie IP. Kable UTP dla systemu CCTV projektować w innym kolorze niż sieć główna.

System należy okablować zgodnie z wytycznymi producenta.

Rejestrator wraz okablowaniem należy zainstalować w dedykowanej szafie w serwerowni. Podgląd za pomocą sieci komputerowej oraz stanowiska komputerowego z zainstalowaną dedykowaną aplikacją.

Ostateczną lokalizację i ilość kamer uzgodnić z Inwestorem na etapie projektu wykonawczego.

Do monitoringu należy dodać monitor poglądowy w serwerowni nie mniejszy niż 32"

Monitory do pracy ciągłej minimum 50" dedykowane do systemów CCTV do pracy ciągłej w trybie 24h/7dni, podgląd /monitor/ w pomieszczeniu wskazanym przez użytkownika.

Ilość monitorów: 1sztuka/24 kamery

Zapis rejestracji nagrań na dysku powinien obejmować minimum 30 dni zapisu ciągłego przy ilości klatek 15kl/s.

Założenia:

- poziom odniesienia jakościowego i cenowego sprzętu: sprzęt CCTV firm Hikvision, Dahua lub równoważny;

- rejestracja obrazu w rejestratorach cyfrowych, z zestawem dysków twardych o pojemności wystarczającej na rejestrację zdarzeń z podłączonych kamer w okresie min. 30 dni, z wbudowaną nagrywarką DVD, wejściem LAN RJ45 i USB;
- kamery zewnętrzne montowane na budynku, dzień/noc, min. 6 Mpix, stacjonarne;
- kamery przy wejściu głównym do budynku – dzień/noc, min. 4 Mpix, z oświetlaczem poczerwieni, kompaktowe lub kopułkowe;
- kamera w pomieszczeniu serwerowni, mag. dowodów wielkogabarytowych, mag. przejściowym, mag. laboratorium – wewnętrzna, szerokokątna, typu dzień/noc, z oświetlaczem podczerwieni, min. 4 Mpix, kopułkowa;
- kamery przy wejściu do kancelarii tajnej, archiwum, magazynku broni – wewnętrzne, dzień/noc, min. 4 Mpix, kopułkowe;
- korytarze – kamery kopułkowe, dzień/noc, min. 4 Mpix;
- kamery w pokoju okazań, przesłuchań – wewnętrzne, szerokokątne, kolor, min 4 Mpix;
- na stanowiskach nadzoru monitoringu przewiduje się montaż monitorów oraz konsoli operatorskiej, myszy;

4. Zasilanie infrastruktury IT.

4.1. Pomieszczenie dla urządzeń zasilania bezprzerwowego.

Urządzenia zasilania bezprzerwowego umieścić w pomieszczeniu rozdzielni głównej (RG) i wyposażać w klimatyzację. Należy zaprojektować pomieszczenie o pow. ok. 30 m² dla siłowni telekomunikacyjnej i UPS z bateriami akumulatorów, rozdzielni elektrycznych i innych z jednoskrzydłowymi drzwiami pożarowymi EI60 o szerokości 100cm i wysokości 220cm.

– w pomieszczeniu tym należy zaprojektować system klimatyzacji precyzyjnej redundantnej N+N (moc chłodnicza pojedynczej jednostki to 5kW). Pomieszczenie bez podłogi technicznej i bez sufitu podwieszanego.

– rozdzielnica elektryczna powinna zapewnić zasilanie urządzeń serwerowni napięciem stałym i przemiennym z siłowni telekomunikacyjnej, centralnego UPS’a oraz napięciem ogólnym z sieci ogólnej;

4.2. Siłownia telekomunikacyjna.

W projekcie przewidzieć zakup i montaż siłowni telekomunikacyjnej prostownikowo-inwerterowej o konstrukcji modułowej N+1:

- o mocy min 5kW dla DC, z możliwością rozbudowy o kolejne moduły do 30kW,
- o mocy min 20kVA dla AC z możliwością rozbudowy o kolejne moduły do 30kVA,
- Dwie baterie akumulatorów 48V o pojemności min. 1000 Ah każda (wymagany czas podtrzymania bateryjnego 3h)

w zakresie:

- dostawa, instalacja i uruchomienie siłowni prostownikowo-inwerterowej,

- dostawa, instalacja i uruchomienie baterii akumulatorów wraz z niezbędnymi elementami do ustawienia, montażu i podłączenia baterii do siłowni prostownikowej;
- szkolenie z zakresu obsługi instalowanych systemów zasilania;
- wykonanie dokumentacji projektowej, technicznej i powykonawczej;

Baterie akumulatorów wg klasyfikacji Eurobatu „Long Life”, żywotność projektowana min. 15 lat.

Siłownia telekomunikacyjna, musi zasilać bezprzerwowo wszystkie urządzenia teleinformatyczne w pomieszczeniu serwerowni, newralgiczne dla działania jednostki urządzenia teleinformatyczne oraz w razie ich zaprojektowania Pomocnicze Punkty Dystrybucyjne sieci, bądź inne pomieszczenia dla potrzeb łączności. Siłownia powinna zapewnić minimum trzygodzinne podtrzymanie pracy urządzeń łączności. Siłownia powinna być zasilana z odrębnego, rezerwowanego agregatem prądotwórczym pola rozdzielnic głównej RG.

Wyłączanie pożarowe źródeł za pomocą wyniesionego "głównego wyłącznika prądu" siłowni prostownikowej 48VDC wraz z odłączeniem baterii i siłowni inwertorowej 230VAC.

Zarządzanie siłownią:

- lokalne poprzez wybieranie za pomocą przycisków na sterowniku z wyświetlaczem LCD;
- zdalne przez TCP/IP lub SNMP za pomocą dedykowanej aplikacji dostarczonej do zarządzania siłownią (dopuszcza się odczyt informacji z siłowni za pomocą przeglądarki sieci Web np. Internet Explorer).
- podłączenie siłowni do systemu nadzoru TelWin za pomocą protokołu TCP/IP poprzez istniejącą sieć LAN lub SNMP w celu przekazywania informacji o parametrach i stanach alarmowych systemu zasilania. Należy dokonać niezbędnej rozbudowy stanowiska nadzoru do monitorowania i nadzorowania stanów dostarczonych siłowni poprzez zwiększenie ilości jednocześnie monitorowanych obiektów polegającej np. na dokupieniu licencji (po rozbudowie funkcjonalność systemu nadzoru TelWin ma być równoważna lub większa z obecnie nadzorowanymi siłowniami).

Uwaga : kabel energetyczny zasilający siłownię projektować z zapasem, umożliwiającym zwiększenie poboru mocy o 50%.

4.3. Zasilanie gwarantowane - UPS.

W celu zapewnienia bezprzerwowego zasilania należy zaprojektować centralny obiektowy UPS na potrzeby funkcjonowania placówki, uwzględniając zasilanie urządzeń komputerowych wymagających zasilania gwarantowanego o mocy 30kVA. UPS wyposażać w zewnętrzny ręczny bajpas serwisowy. Wymaga się, aby UPS był o konstrukcji modułowej przy założeniu, iż przynajmniej jeden moduł jest rezerwowany (

n+1). UPS musi umożliwiać rozbudowę o kolejne moduły. Czas podtrzymania zasilania dla gniazd DATA oraz sieci LAN – 15 minut.

Do zasilania urządzeń w pomieszczeniach open-space 0.32 i 0.42 zaprojektować dedykowany zasilacz UPS o konstrukcji modułowej z zasadą redundancji n+1 o mocy dostosowanej do mocy zasilanych urządzeń i czasie podtrzymania zasilania 15 minut.

W projektach konstrukcyjnych budynku należy uwzględnić **zwiększone obciążenie stropów i posadzek pod UPS'em i siłownią telekomunikacyjną.**

5. Pozostałe systemy i instalacje

5.1. System sygnalizacji włamania i napadu SSWiN.

System sygnalizacji włamania objąć wszystkie otwory okienne i drzwiowe pomieszczeń na poziomie parteru oraz 1 piętra, a ponadto wymagalny jest system SSWiN dla pomieszczeń magazynu uzbrojenia, archiwów, kancelarii tajnej, serwerowni itp.

Zastosować mikroprocesorową centrale alarmową min Grade 3, wyposażoną w niezbędny zasilacz, w niezbędne kart funkcyjne, interfejsy sterujące i transmisyjne, panel wyświetlacza w języku polskim. Zasilanie z wydzielonego obwodu zasilania bezprzerwowego z siłowni telekomunikacyjnej o napięciu 230V. Zasilanie awaryjne systemu poprzez akumulator żelowy o odpowiedniej pojemności, zgodnie z wymaganym czasem pracy awaryjnej, zapewniającej prawidłową pracę systemu w stanie dozoru przez minimum 24 godz. bez zasilania podstawowego, oraz po upływie tego czasu minimum 0,5 godz. w stanie alarmowania.

Manipulator LCD zlokalizowany przy wejściu głównym do wydzielonych stref, ciekłokrystaliczny, pozwalający na poruszanie się po funkcjach dostępnych z poziomu użytkownika. Rozbrojenie i zazbrojenie poprzez manipulatory.

System włączyć do sieci LAN umożliwiając zdalne monitorowanie.

Centrala alarmowa zlokalizowana w pomieszczeniu o ograniczonym dostępie np. pom. serwerowni.

Pomieszczenie serwerowni powinno zostać traktowane jako osobna strefa dozoru instalacji SSWiN.

5.2. System kontroli dostępu SKD.

Zaprojektować instalację kontroli dostępu opartą o system pracujący w standardzie ACCO NET zapewniający funkcjonalność oraz umożliwiający zarządzanie nim bezpośrednio przez sieć LAN/WAN dzięki wbudowanemu interfejsowi Ethernet.

Karty dostępowe UNIQUE 125kHz dostarczy Wykonawca.

Zaprojektować przejścia kontrolowane jednostronnie / dwustronne we wszystkich pomieszczeniach poza aneksami ksero, niszczarniami, pomieszczeniami socjalnymi, pokojami sprzątaczek, zabezpieczające przed dostępem osób nieupoważnionych do budynku, grup pomieszczeń oraz wybranych pomieszczeń technicznych. Każde drzwi wyposażone w kontrolę dostępu należy wyposażyć w samozamykacz drzwiowy. Przyjęte rozwiązanie powinno uniemożliwiać otwarcie pomieszczeń w przypadku braku zasilania, lecz umożliwiać ewakuację z pomieszczenia w przypadku zagrożenia pożarowego.

Dobre kontrolery wyposażać w klawiaturę oraz wbudowany czytnik EM125kHz.

Projektowany system kontroli dostępu należy połączyć za pomocą interfejsu komunikacyjnego RS485/RS232 oraz odpowiedniego modułu z centralą systemu sygnalizacji włamania i napadu. Integracja systemów umożliwi sterowanie uzbrojeniem stref alarmowych zarówno z poziomu manipulatorów systemu alarmowego jak i czytników systemu kontroli dostępu. Dodatkowym atutem takiego rozwiązania jest zbieranie przez centralę SKD w logu krytycznych zdarzeń pochodzących z systemu alarmowego.

Drzwi objęte kontrolą dostępu należy wyposażać w zwory elektromagnetyczne 540 kg oraz kontaktrony monitorujące ich stan (zamknięte / otwarte).

Wszystkie drzwi objęte systemem SKD powinny mieć możliwość awaryjnego otwarcia przyciskiem awaryjnego otwierania oraz kluczem w przypadku braku klamki.

Skrzynki depozytowe kluczy dla poszczególnych pokoi oraz osobne skrzynki depozytowe na klucze do samochodów należy wyposażać w czytniki kart tego samego producenta co instalacji kontroli dostępu dla budynku. Stan każdej skrytki powinien zostać zwizualizowany w dedykowanym oprogramowaniu na komputerze wskazanym przez użytkownika obiektu – osobno dla skrytek pokoi, osobno dla skrytek kluczy do samochodów.

Pomieszczenia serwerowni oraz siłowni telekomunikacyjnej wyposażać w dwustronną kontrolę dostępu.

5.3. System sygnalizacji pożaru SSP.

Projektowany budynek administracyjno-biurowy będzie posiadał 3 kondygnacje nadziemne (brak podpiwniczenia). W świetle przepisów z zakresu ochrony przeciwpożarowej budynek ten należy kwalifikować jako budynek niski ZL III.

UWAGA: poniższe założenia stanowią wstępne wytyczne, określenie ostatecznych warunków ochrony przeciwpożarowej należy do projektanta opracowującego Projekt Budowlany, w porozumieniu z Rzeczoznawcą.

Biorąc pod uwagę przeznaczenie obiektu należy wyposażać go w instalację SSP za wyłączeniem pomieszczeń mokrych wyposażonych w natryski – zgodnie z obowiązującymi przepisami. Instalacją SSP należy również objąć budynek garażowy.

Przestrzeń międzystropowe przez które przebiegają instalacje bezpieczeństwa należy również wyposażać w czujki dymu.

W budynku należy zainstalować nową centralę systemu sygnalizacji pożaru w pomieszczeniu stałego przebywania przeszkolonego personelu na poziomie parteru. Pomieszczenie to należy wyposażać w czujki dymu oraz przycisk ROP umiejscowiony w pobliżu centrali CSP. Odcinki linii kablowych, które przebiegają przez strefy nie objęte ochroną systemu SSP należy wykonać w odporności ogniowej E90 na certyfikowanych trasach kablowych.

Sposób pracy instalacji systemu pożaru powinien być zgodny ze scenariuszem pożarowym przyjętym dla opracowywanego budynku.

System sygnalizacji pożaru powinien spełniać standardy bezpieczeństwa w zakresie kompleksowego dozoru przeciwpożarowego.

System wykrywania i sygnalizacji pożaru powinien składać się z:

- centrali wykrywania i sygnalizacji pożaru – CSP,
- czujek dymu,
- przycisków pożarowych – ROP,
- wysokonapięciowych modułów wejść/wyjść,
- okablowania czujek oraz urządzeń związanych z instalacją SSP,
- sygnalizatorów akustycznych.

Instalację wykonać w postaci linii dozorowej (pętli), która zaczyna i kończy się w centrali sygnalizacji pożaru (CSP). Instalacja adresowalna, pracująca w układzie dialogowym, gwarantującą wysoką niezawodność i jakość funkcjonowania.

System sygnalizacji pożaru będzie współpracował z urządzeniami pomocniczymi:

- urządzeniami wentylacyjnymi,
- dźwigami,
- kontrolą dostępu,
- centralą oddymiania
- zaworem pierwszeństwa.

System sygnalizacji pożaru połączyć z w/w systemami za pomocą modułów i adapterów zamontowanych na linii dozorowej. Pomiędzy systemami będą przekazywane informacje o alarmie, stanie pracy urządzeń, oraz będzie możliwość sterowania.

W przypadku wykrycia pożaru zostanie przerwane zasilanie elektrozaczepów i zwór magnetycznych drzwi objętych kontrolą dostępu. Elektrozaczepy rewersyjne muszą zostać zwolnione w celu umożliwienia ewakuacji osób ze stref objętych zagrożeniem pożarowym.

W przypadku wykrycia pożaru muszą zostać wyłączone urządzenia wentylacyjne, zamknięte odcinające kłapy pożarowe na kanałach wentylacyjnych. w celu uniemożliwienia rozprzestrzeniania się dymu po innych strefach pożarowych.

Czujki montować w pomieszczeniach do sufitu podwieszanego oraz w przestrzeniach międzysufitowych. Dobór typu czujek oraz ich rozmieszczenie dobrać po uwzględnieniu geometrii pomieszczenia: tj. powierzchni, kształtu, typu stropu, wysokości zgodnie, z wytycznymi CNBOP.

Ręczne ostrzegacze pożaru ROP montowane będą: w części korytarzowej, przy przejściach przez strefy pożarowe, na klatkach schodowych, hydrantach oraz przy drzwiach ewakuacyjnych. ROP należy montować na wysokości 1,6m od poziomu podłogi.

Okablowanie

Linie dozоровe (pętle) należy wykonać przewodem typu YnTKSYekw 1x2x0,8, a przewody które muszą funkcjonować przez więcej niż 1min po wykryciu pożaru powinny być odporne na oddziaływanie ognia przez 90min (sterowanie urządzeniami pożarowymi).

Trasy kablowe przechodzące przez ściany wydzieleni pożarowych należy zabezpieczyć masą ogniochronną do klasy ochrony danej przegrody.

Jeżeli do połączeń w obwodach sygnalizacji pożarowej stosuje się kable wielożyłowe, to żadna z żył nie może być używana w obwodach innych niż obwody sygnalizacji pożarowej.

Zasilanie

Centralę sygnalizacji pożaru zasilic z sekcji pożarowej rozdzielnicy głównej RG budynku sprzed wyłącznika głównego. Centrala musi posiadać zasilanie awaryjne (z akumulatorów), które umożliwi pracę instalacji w przypadku awarii zasilania podstawowego przez czas 72 godzin oraz zapewni 30 minut pracy w stanie alarmowania.

Oznaczenia

Wszystkie kable, czujki, ROP-y, przekaźniki powinny być oznaczone numerycznie, w sposób trwały. Te same oznaczenia powinny mieć odzwierciedlenie w CSP.

Wszystkie zastosowane do budowy elementy instalacji (przewody, kable, urządzenia), powinny posiadać ważny certyfikat zgodności do stosowania w ochronie przeciwpożarowej, wydawane przez Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej w Józefowie k/Otwocka.

Instalacja wizualizacji zdarzeń w punkcie nadzoru

W pomieszczeniu punktu nadzoru, np. Dyżurce OPP, należy zainstalować monitory umożliwiające podgląd instalacji CCTV oraz naruszenia stref SSWIN. Instalacje te powinny współgrać ze sobą w celu umożliwienia szybkiej lokalizacji intruza na terenie obiektu.

W pomieszczeniu tym należy zainstalować panel wyniesiony oraz komputer z oprogramowaniem umożliwiającym wizualizację miejsca wystąpienia zagrożenia pożarowego.

W obiekcie należy zaprojektować indywidualną instalację sygnalizacji alarmu pożaru.

Ochronie podlegać powinny:

- magazyny i składnice akt, dowodów rzeczowych, sprzętu policyjnego, broni;
- pomieszczenie kancelarii tajnej, archiwum, przetwarzania informacji niejawniej;
- pomieszczenia łączności i informatyki (serwerownia, siłownia telekomunikacyjna, UPS),
- przestrzenie międzysufitowe w przypadku zastosowania sufitów podwieszanych.

Centralę alarmową sygnalizacji pożaru należy umieścić w pomieszczeniu nadzoru.

Instalacja oddymiania klatek schodowych

W budynku przewiduje się instalację oddymiania klatek schodowych. Centralę oddymiania należy podłączyć do instalacji systemu sygnalizacji pożaru. Sygnał o zagrożeniu pożarowym zostanie przesłany na wejście wyzwalające centrali oddymiania z systemu SSP. Do centrali instalacji oddymiania należy podłączyć przyciski oddymiania, które bezzwłocznie aktywują proces oddymiania klatki schodowej oraz wysłać sygnał alarmu pożarowego do instalacji SSP. Instalacja SSP również musi monitorować stany alarmowe centrali oddymiania.

Centralę oddymiania należy zasilic z sekcji odbiorów pożarowych rozdzielni głównej budynku kablami o odporności ogniowej 90 minutowej na certyfikowanych trasach kablowych.

Sposób pracy centrali oddymiania powinien być zgodny ze scenariuszem pożarowym przyjętym dla opracowywanego budynku.

5.4. Instalacja odbiorcza RTV

W obiekcie należy przewidzieć instalację odbiorczą kablową TV naziemnej, z antenami na dachu budynku i gniazdami przyłączeniowymi RTV w Sali Odpraw i pokojach naczelników wydziałów.

5.5. Instalacje audiowizualne

System audio-wideo zaprojektować w salach odpraw i sali operacyjnej/sztab.

W pomieszczeniach gdzie zostanie zainstalowany system AV projektować sterowanie natężenia oświetlenia roletami, oraz obsługę projektora z poziomu pulpitu.

5.6. Instalacje audiowizualne w pom. przesłuchań

Odrębny system audio – wideo z odrębnym rejestratorem, umożliwiający zapis obrazu i głosu osób okazywanych. Dodatkowo interkom dwukierunkowy do komunikacji pomiędzy sąsiednimi dwoma pomieszczeniami.

5.7. Instalacja wideodomofonowa

W budynku przewiduje się instalacje wideodomofonowe w standardzie IP. Przed wejściami do pomieszczeń 0.32, 0.42 oraz przed wybranymi wejściami do budynku należy zainstalować panele wywoławcze wideodomofonu. Monitory odbiorcze w ww. pomieszczeniach oraz w centralnym punkcie nadzoru, np. Dyżurce na terenie OPP. Monitory odbiorcze kolorowe o przekątnej minimum 7'', powinny umożliwiać komunikację głosową oraz wizyjną z osobą stojącą przed stacją wywoławczą oraz umożliwić zwolnienie elektrozwoły drzwi.

5.8. Instalacja przyzywowa

W pomieszczeniach WC NSP dla niepełnosprawnych przewidzieć zastosowanie przycisku przywoławczego umożliwiającego przywołanie personelu. Przy drzwiach od strony pomieszczenia należy zlokalizować przycisk kasująco odwoławczy wezwanie. Na zewnątrz pomieszczenia, nad drzwiami zamontować lampkę sygnalizacyjną z buczkiem. Przywołanie z pomieszczeń WC dla NSP należy doprowadzić do pomieszczenia wskazanego przez użytkownika obiektu.

5.9. Automatyka bramy wjazdowej

Bramę wjazdową do jednostki wyposażać w domofon oraz w system automatycznego otwierania bramy za pomocą pilota odbiornika radiowego, a także przyciskiem ze stanowiska wskazanego przez użytkownika.

5.10. Ochrona elektromagnetyczna pomieszczeń

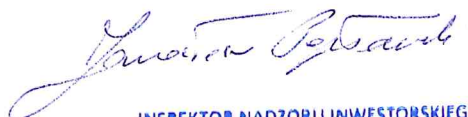
Z uwagi na przetwarzanie oraz dostęp do informacji niejawnych w pomieszczeniach 0/32 i 0/42 zlokalizowanych w projektowanym budynku, wymagane jest zapewnienie zgodnego z przepisami poziomu ochrony elektromagnetycznej tych pomieszczeń. Na etapie opracowania dokumentacji projektowej należy przeanalizować i dobrać odpowiednie rozwiązania projektowe.

Uwaga:

1. Instalacje niskoprądowe w pomieszczeniach zaprojektować jako podtynkowe, w peszlach lub rurkach PCV, a główne ciągi kablowe w systemie natynkowym z zachowaniem 25% rezerwy na rozbudowę.
2. Do miejsc instalacji central alarmowych, kontrolerów systemu kontroli dostępu, urządzeń monitoringu wizyjnego - należy doprowadzić instalacje zasilające z odpowiednim napięciem.
3. **Zasilanie centrali SSP projektować z przed wyłącznika ppoż zasilania budynku.**
4. Wymagania standaryzacyjne dotyczące systemów zasilania bezprzerwowego i rezerwowego zawarte są w dokumentach p.t. "Zalecenia dotyczące standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności" z dnia 10.12.2013r. oraz "Wymagania dotyczące standardów technicznych, użytkowych oraz bezpieczeństwa, stosowanych w Policji w zakresie informatyki i łączności" opracowanie ze stycznia 2020r.

Oprac. J.P.

ZASTĘPCA NACZELNIKA
WYDZIAŁU ŁĄCZNOŚCI I INFORMATYKI
KWP w Gdańsku
Ryszard Bednarek


INSPEKTOR NADZORU INWESTORSKIEGO
Komenda Wojewódzka Policji w Gdańsku
mgr inż. Jarosław POPLAWSKI
upr. bud. nr POM/0370/PWBT/19
w specjalności instalacyjnej w zakresie sieci, instalacji
i urządzeń telekomunikacyjnych
w zakresie kierowania robotami budowlanymi
bez ograniczeń

