

DOKUMENTACJA TECHNICZNA

Modernizacja systemu monitoringu wizyjnego oraz kontroli dostępu w budynku Prokuratur poznańskich przy ulicy Solnej 10 w Poznaniu

ZAKRES OPRACOWANIA: Dokumentacja techniczna

NAZWA INWESTYCJI: Modernizacja systemu monitoringu wizyjnego oraz kontroli dostępu w budynku Prokuratur poznańskich przy ulicy Solnej 10 w Poznaniu

INWESTOR: Prokuratura Okręgowa
ul. Solna 10
61-736 Poznań

JEDNOSTKA PROJEKTOWA: Przedsiębiorstwo Handlowo-Usługowe
NET KOM Tomasz Klemenski
Ul. Prosta 9, 64-000 Kościan, NIP 6981548828

Stanowisko	Imię i nazwisko	Data	Podpis
Projektant	mgr inż. Tomasz Klemenski (Uprawnienia budowlane do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności telekomunikacyjnej, przewodowej i radiowej wraz z infrastrukturą towarzyszącą nr ewidencyjnej WKP/0297/PWOT/06)	07.2026 r.	

Poznań, lipiec 2026

1. Spis treści

1.	Spis treści.....	2
2.	Dane inwestycji	3
2.1	Inwestor.....	3
2.2	Adres inwestycji	3
2.3	Wspólny słownik zamówień (CPV)	3
2.4	Podstawa opracowania	3
3.	Zakres opracowania	3
4.	Inwentaryzacja systemu.....	4
5.	Analiza możliwości.	5
6.	Opis techniczny	7
6.1	System nadzoru video CCTV/VSS oraz integratora SKD/SSWiN/SSP	7
6.1.1	Informacje ogólne	7
6.1.2	Cyberbezpieczeństwo:	8
6.1.3	Wymagania dla systemu CCTV - Zgodność z RODO/bezpieczeństwo.....	9
6.1.4	Parametry funkcjonalne systemu:	10
6.1.5	Minimalne parametry dla stacji klienckich:	15
6.1.6	Minimalne parametry dla stosowanych serwerów:	16
6.1.7	Minimalne parametry dla stosowanych macierzy:	16
6.1.8	Minimalne parametry dla stosowanych kamer tubowych:	17
6.1.9	Minimalne parametry dla stosowanych kamer kopułowych:.....	18
6.1.10	Minimalne parametry dla stosowanych kamer obrotowych:.....	19
6.1.11	Minimalne parametry dla stosowanych przełączników sieciowych:	19
6.2	Opis integracji z systemami VSS, KD, SSWIN, SAP	21
6.3	Opis bramki obrotowej.....	24
7.	Zagadnienia BHP, normy	26
8.	Wytyczne dla Wykonawców	27
9.	Kosztorys Inwestorski i przedmiar robót.	28

2. Dane inwestycji

2.1 Inwestor

Prokuratura Okręgowa

ul. Solna 10

61-736 Poznań

2.2 Adres inwestycji

Budynki Prokuratury Okręgowej w Poznaniu położone przy ul. Solna 10, 61-736 Poznań

2.3 Wspólny słownik zamówień (CPV)

35121700-5

32323500-8

71320000-7

51312000-2

2.4 Podstawa opracowania

- Umowa z Inwestorem,
- Uzgodnienia z Inwestorem,
- Obowiązujące akty prawne i normy,
- Inwentaryzacja budynku i systemów elektronicznej ochrony,
- Dokumentacja powykonawcza istniejących systemów elektronicznej ochrony,
- Wizja lokalna,
- Dane zebrane przez projektanta,

3. Zakres opracowania

Przedmiotem opracowania jest dokumentacja techniczna dla zadania: „Modernizacja systemu monitoringu wizyjnego oraz kontroli dostępu w budynku Prokuratur poznańskich przy ulicy Solnej 10 w Poznaniu” wraz z kosztorysem inwestorskim.

Dokumentacja techniczna obejmuje: inwentaryzację systemu, analizę możliwości modernizacji i rozbudowy, kosztorys inwestorski i przedmiar robót, wytyczne dla Wykonawców.

Dokumentacja techniczna została wykonana w zgodnie z zasadami wiedzy technicznej oraz normami prawnymi.

Niniejsza dokumentacja techniczna nie jest projektem architektoniczno-budowlanym ani projektem technicznym w myśl ustawy Prawo Budowlane, a jedynie stanowi podstawę do ich sporządzenia

Kosztorys inwestorski i przedmiar robót wskazują ilości urządzeń oraz robót (znane na dzień sporządzenia opracowania), które będzie należało zaprojektować i wykonać.

Na etapie projektowania może wystąpić konieczność zmiany ilości urządzeń bądź ich lokalizacji.

Ze względu na charakter obiektu i jawność niniejszego opracowania nie wskazuje ono dokładnych lokalizacji urządzeń. Wykonawca zapozna się ze szczegółami po podpisaniu odpowiednich oświadczeń o zachowaniu poufności. Obiekt posiada dokumentację powykonawczą zamontowanych urządzeń i instalacji.

4. Inwentaryzacja systemu.

W ramach inwentaryzacji istniejącego systemu monitoringu wizyjnego przeprowadzono kompleksowe działania mające na celu ustalenie aktualnego stanu technicznego instalacji oraz określenie elementów możliwych do wykorzystania w modernizowanym systemie.

W pierwszej kolejności dokonano przeglądu wszystkich funkcjonujących kamer, obejmującego ich lokalizację, stan techniczny, parametry optyczne oraz jakość generowanego obrazu. W ramach inwentaryzacji istniejącego systemu monitoringu wizyjnego również zweryfikowano, czy istniejące urządzenia spełniają wymagania w zakresie cyberbezpieczeństwa określone w ustawie o Krajowym Systemie Cyberbezpieczeństwa. Ocenie podlegał w szczególności producent kamer, ich oprogramowanie układowe, dostępne mechanizmy zabezpieczeń oraz zgodność z aktualnymi standardami ochrony danych.

Sprawdzono, czy urządzenia posiadają aktualne i wspierane wersje firmware, czy umożliwiają stosowanie bezpiecznych protokołów komunikacyjnych, a także czy oferują

funkcje takie jak szyfrowanie transmisji, kontrola dostępu, ochrona przed nieautoryzowaną konfiguracją oraz możliwość prowadzenia audytu zdarzeń. Weryfikacja ta jest niezbędna, aby określić, czy istniejące kamery mogą zostać pozostawione w modernizowanym systemie, czy też wymagają wymiany na modele zgodne z obowiązującymi wymogami KSC.

Dokonano oceny istniejących tras kablowych, rodzaj zastosowanego okablowania oraz jego stan, w celu określenia, czy infrastruktura ta może zostać wykorzystana ponownie, czy wymaga wymiany lub dostosowania do nowych standardów transmisji danych.

5. Analiza możliwości.

Na potrzeby niniejszej dokumentacji została przeprowadzona analiza możliwości modernizacji systemu monitoringu wizyjnego oraz kontroli dostępu w budynku Prokuratury poznańskich przy ulicy Solnej 10 w Poznaniu, a także pozostałych systemów bezpieczeństwa technicznego.

Analiza możliwości elektronicznych systemów ochrony obejmuje ocenę warunków technicznych, środowiskowych oraz funkcjonalnych, które determinują zakres i sposób wdrożenia lub modernizacji systemu na terenie obiektu. Jej celem jest określenie, jakie funkcje, parametry oraz poziom działania systemu mogą zostać realnie osiągnięte w danych warunkach, tak aby zapewnić zgodność z wymaganiami użytkownika oraz efektywność późniejszej eksploatacji. Na tym etapie analizowane są istniejące instalacje teletechniczne i systemy bezpieczeństwa, takie jak CCTV, SSWiN, SSP, kontrola dostępu czy BMS, które mogą zostać zintegrowane z monitoringiem wizyjnym w celu rozszerzenia jego funkcjonalności. Równocześnie oceniane są warunki instalacyjne, obejmujące dostępność infrastruktury, możliwości prowadzenia okablowania oraz lokalizację punktów montażowych, co pozwala określić techniczne ograniczenia i potencjał systemu.

Istotnym elementem analizy jest dobór technologii, w tym określenie typów kamer, które mogą zostać zastosowane w monitorowanych obszarach — kamer stacjonarnych, obrotowych PTZ oraz ocena ich przydatności w kontekście zakładanych celów nadzoru. Równolegle analizowana jest kompatybilność z oprogramowaniem VMS, które będzie odpowiadać za zarządzanie nagraniami, ich archiwizację oraz analizę, a także możliwości integracji monitoringu z innymi systemami bezpieczeństwa, takimi jak system alarmowy, kontrola

dostępu czy system sygnalizacji pożaru. W ramach analizy określa się również skalowalność systemu, czyli potencjał jego rozbudowy o dodatkowe kamery, zwiększenie przestrzeni dyskowej czy rozszerzenie funkcji analitycznych. Ważnym aspektem jest także bezpieczeństwo danych, obejmujące mechanizmy szyfrowania, kontrolę dostępu, redundancję oraz ochronę przed nieautoryzowanym dostępem. Ostatecznie oceniana jest efektywność działania, czyli zdolność systemu do wspierania służb porządkowych poprzez szybkie reagowanie na zdarzenia, ułatwioną weryfikację materiału dowodowego oraz zwiększenie ogólnego poziomu bezpieczeństwa na terenie obiektu.

Po wykonaniu inwentaryzacji i analizy stwierdzono:

- Istniejący system CCTV jest dość stary, jego jakość jest niewystarczająca, sprzęt jest zużyty, bez gwarancji, brak możliwości aktualizacji oprogramowania
- Konieczność wymiany kamer na nowe w technologii IP
- Konieczność wymiany rejestratorów i systemu zarządzania na nowy w technologii IP
- Możliwość wykorzystania istniejącego okablowania koncentrycznego do kamer poprzez zastosowanie konwerterów
- Możliwość zainstalowania oprogramowania integrującego systemy CCTV, SKD, SSWIN i SSP. Możliwość zarządzania ww. systemami z poziomu jednego oprogramowania.
- Nowe oprogramowanie integrujące może obsługiwać istniejące na obiekcie systemy SKD, SSP, SSWIN
- Konieczność dostosowania systemów do wymagań cyberbezpieczeństwa
- Konieczność wymiany bramek obrotowych w holu głównym budynku.

6. Opis techniczny

6.1 System nadzoru video CCTV/VSS oraz integratora SKD/SSWiN/SSP

6.1.1 Informacje ogólne

Dokumentacja Techniczna (DT) przewiduje modernizację systemu nadzoru wizyjnego zapewniającego rejestrację obrazu i dźwięku oraz wizualizację obrazu z kamer na dedykowanych stanowiskach.

DT przewiduje również integrację systemu nadzoru wizyjnego z istniejącym systemem sygnalizacji włamania i napadu, istniejącym systemem kontroli dostępu oraz istniejącym systemem sygnalizacji pożarowej.

Rejestracja obrazu oraz dźwięku ma odbywać się na serwerach rejestrujących z zainstalowanym oprogramowaniem serwerowym. Prowadzony będzie z szybkością 25kl/s dla wszystkich kamer. Serwer rejestrujący należy umieścić w pomieszczeniu administratora przy stanowisku ochrony.

Stacje klienckie umieszczone zostaną w pomieszczeniu ochrony nr1, nr 2 oraz w pomieszczeniu administratora.

Pośrednia szafa dystrybucyjna zlokalizowana zostanie w pomieszczeniu kancelarii niejawnej.

Na potrzeby systemu należy zaprojektować dwie nowe szafy Rack 19" 42U, jedna jako pośredni punkt dystrybucyjny zlokalizowany w pomieszczeniu kancelarii niejawnej oraz druga szafa Rack 19" 42U jako główny punkt dystrybucyjny zlokalizowany w pomieszczeniu administratora.

W pośrednim punkcie dystrybucyjnym należy zastosować konwertery sygnału analogowego na sygnał cyfrowy istniejących kamer systemu monitoringu.

Szafę PPD oraz GPD należy połączyć ze sobą dwoma kablami światłowodowymi SM min. 4J.

Zamawiający wymaga dostarczenia systemu nadzoru wizyjnego wraz z serwerami z wbudowanymi macierzami RAID oraz macierzą RAID zapewniającą pracę w środowisku klastra wysokiej dostępności.

System musi zapewniać obsługę i archiwizację min. 100 kanałów wideo w ramach dostarczonej licencji. Serwery należy wyposażyć w dwa dyski SSD („minimalne parametry dla stosowanych urządzeń rejestrujących”).

Macierz należy wyposażyć w dyski do pracy ciągłej o łącznej pojemności zapewniającą archiwizację materiału wideo przez okres 30 dni.

Na potrzeby systemu planuje się nowe stacje robocze wyposażone w mysz i klawiaturę oraz cztery monitory 32” w pomieszczeniach ochrony.

W pomieszczeniu administratora projektuje się stację roboczą wyposażoną w mysz i klawiaturę oraz jeden monitor 32” w pomieszczeniach ochrony.

W każdym z punktów dystrybucyjnych należy zainstalować zasilacze typu UPS, zapewniające awaryjne zasilanie podłączonych do niego urządzeń w przypadku utraty zasilania gwarantowanego na okres minimum 30 minut.

W każdym z pomieszczeń gdzie zlokalizowane są stacje klienckie należy zainstalować zasilacze typu UPS, zapewniające awaryjne zasilanie podłączonych do niego urządzeń w przypadku utraty zasilania gwarantowanego na okres minimum 10 minut.

6.1.2 Cyberbezpieczeństwo:

Wymaga się stosowania rozwiązań technologicznych pochodzących z krajów UE, EOG lub NATO, Urządzenia oraz oprogramowanie muszą spełniać aktualne wymagania w zakresie bezpieczeństwa informacji, w tym pozostawać w zgodności z regulacjami:

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, NIS2 oraz CER.

W szczególności nie dopuszcza się wykorzystania urządzeń od producentów, którzy w niektórych państwach członkowskich UE zostali objęci ograniczeniami w zakresie stosowania

rozwiązań w sektorze publicznym, infrastrukturze krytycznej, wojsku, służbach lub szkolnictwie.

Producent kamer do monitoringu CCTV musi spełnić poniższe wymagania, które mogą pomóc organizacjom w zwiększeniu ich cyberbezpieczeństwa w celu zapewnienia zgodności z Ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw:

- bezpieczeństwo z punktu widzenia łańcucha dostaw (Supply Chain Security),
- zastosowanie dobrych praktyk – wybór rozwiązań bezpiecznych (hardware),
- zarządzanie cyklem życia: regularne aktualizacje firmware'u (łatki bezpieczeństwa) gwarantowane przez producenta,
- szyfrowanie end-to-end: Zapewniają bezpieczną transmisję danych przy użyciu protokołów TLS/HTTPS,
- bezpieczne logowanie: Wymuszanie silnych haseł i obsługa certyfikatów cyfrowych,
- możliwość raportowania luk w zabezpieczeniach od niezależnych badaczy, organizacji, dostawców i klientów.
- wbudowane certyfikowane chipsety szyfrujące FIPS/TPM

6.1.3 Wymagania dla systemu CCTV - Zgodność z RODO/bezpieczeństwo

- Architektura systemu w konfiguracji serwer/klient, wszystkie dane takie jak: materiał audio-wideo, dane użytkowników systemu, logi systemowe i alarmowe muszą być przechowywane na odpowiednio zabezpieczonych serwerach zainstalowanych w dedykowanym pomieszczeniu wskazanym przez zamawiającego.
- System musi zapewniać szyfrowane połączenia pomiędzy serwerem, a aplikacjami klienckimi.
- Kodowany transfer danych oraz przechowywanie danych wizyjnych i dotyczących autoryzacji.
- Eksportowany materiał przekazywany instytucjom zewnętrznym musi być zabezpieczony hasłem. Odtworzenie eksportowanego materiału będzie możliwe tylko po podaniu odpowiedniego hasła.

- System musi umożliwiać dostęp do pełnej funkcjonalności systemu po podaniu haseł dwóch użytkowników.
- System musi rejestrować w bazie danych, informacje o takich zdarzeniach jak:
 - ✓ nawiązanie połączenia z serwerem przez uprawnionego użytkownika,
 - ✓ wyświetlenie obrazu z kamery w trybie „na żywo”,
 - ✓ archiwizacja materiału audio-wideo na stacji klienckiej lub serwerze,
 - ✓ zapis klatki obrazu na stacji klienckiej,
 - ✓ wydruk klatki.
- System musi umożliwiać anonimizację obrazu przedstawiającego osoby zarejestrowane przez system monitoringu oraz umożliwiać przeglądanie materiału wideo bez funkcji anonimizacji przez użytkowników o właściwych uprawnieniach.

6.1.4 Parametry funkcjonalne systemu:

Całą instalację systemu monitoringu wizyjnego należy wykonać w technologii IP w systemie modułowym umożliwiającym dowolne skalowanie, bazujące na architekturze klient-serwer. System należy wykonać tak, aby stanowił kombinację konstrukcji modułowej i sieciowej transmisji danych, w którym wszystkie funkcje zgrupowano w formie modułów zadaniowych, a w celu komunikacji pomiędzy nimi wykorzystano protokół TCP/IP.

Szeroka gama własności i uprawnień wizualizacyjnych zostanie zdefiniowana w formie profili, które będą przyporządkowane poszczególnym użytkownikom lub ich grupom. Przy każdorazowym uruchomieniu oprogramowania klienckiego po zalogowaniu użytkownika, zostanie automatycznie załadowany profil odpowiadający uprawnieniom danego operatora, co umożliwi sterowanie uprawnieniami, liczbą dostępnych do obsługi kamer, pozycjonowaniem obrazów alarmowych oraz możliwościami wywołania scenariuszy alarmowych niezależnie dla każdego użytkownika lub grupy użytkowników.

Logowanie użytkownika do systemu nadzoru wizyjnego odbywa się po podaniu hasła odpowiedniego dla danego konta użytkownika systemu monitoringu wizyjnego. Wszelkie zmiany i czynności dokonane przez zalogowanego użytkownika zostaną zarchiwizowane w postaci logów systemowych. Zarządzanie bazą użytkowników, dodawanie nowych, zmiana

haseł odbywać się będzie wyłącznie za pomocą aplikacji klienckiej zarządzanej przez administratora systemu.

Dla każdej z kamer, pracujących w systemie monitoringu wizyjnego, należy skonfigurować indywidualne parametry obrazu takie jak: rozdzielczość obrazu, rodzaj kompresji, poziom kompresji, prędkość zapisu, metoda rejestracji (detekcja ruchu, zapis ciągły, harmonogram, scenariusz). Wszelkie zmiany parametrów kamer wymienione powyżej muszą odbywać się z poziomu aplikacji klienckiej i muszą być przechowywane w postaci logów systemowych.

Dla każdej z kamer należy skonfigurować trzy strumienie wideo: główny 4 Mpx , pierwszy pomocniczy VGA lub D1, drugi pomocniczy 720/1080 p.

Strumienie wideo należy skonfigurować tak aby w trybie wizualizacji system automatycznie dobierał odpowiedni strumień wideo w zależności od rozdzielczości monitorów. Konfiguracja strumieni wideo:

- 1) monitory 4K, 1 kamera - strumień w rozdzielczości 4 Mpx , podział od 4-9 kamer strumień w rozdzielczości 720/1080p, powyżej 9 kamer strumień D1/VGA
- 2) Dla monitorów Full HD - 1 kamera - strumień w rozdzielczości 4Mpx, podział do 4 kamer strumień w rozdzielczości 720/1080p, powyżej 4 kamer strumień D1/VGA

Zmiana rozdzielczości będzie się odbywać dynamicznie, tzn. w przypadku przeniesienia widoku kamer z monitora pracującego w rozdzielczości 4K na monitor o rozdzielczości FullHD system automatycznie przełączy wyświetlane strumienie wideo na niższą rozdzielczość. W przypadku przeniesienia podziału kamer z monitora pracującego w rozdzielczości FullHD na 4K system zmieni automatycznie strumienie na wyższą rozdzielczość.

System nadzoru wizyjnego musi uruchamiać się automatycznie w trybie usługi systemowej po uruchomieniu serwera. System nadzoru video musi zapewniać funkcję automatycznego zapisu awaryjnego, zapewniającego automatyczne przełączenie zapisu oraz udostępniania obrazu z kamer przez serwer awaryjny w czasie nie dłuższym niż 2 min. Po ponownym przywróceniu uszkodzonego serwera do pracy system automatycznie przełącza obsługę kamer na serwer podstawowy z jednoczesną synchronizacją danych wideo.

- Aplikacja serwerowa oraz kliencka 64-bitowa.
- Aplikacja serwerowa oraz kliencka w języku polskim.

-
- Obsługę systemów wieloprocesorowych.
 - Otwarta platforma dla integracji kamer IP wiodących na rynku dostawców.
 - Oprogramowanie serwerowe współpracujące w różnych platformami systemowymi w tym co najmniej, Windows Server 2022, Windows Server 2025, Windows 10, Windows 11
 - Możliwość rozbudowy dzięki architekturze klient/serwer umożliwiającej dystrybucję i skalowalność systemu.
 - Intuicyjny interfejs użytkownika.
 - Zdalna obsługa podłączonych kamer IP z poziomu oprogramowania zarządzającego. Możliwość zmiany parametrów strumieni obrazowych w kamerze z poziomu aplikacji klienckiej systemu nadzoru video

Funkcje usługi serwerowej:

- Integrację cyfrowych kamer wielu producentów.
- Obsługa kodeków MJPEG, H264, H265.
- Możliwość zdefiniowania dla każdej z kamer indywidualnie, rodzaju kodowania, prędkości transmisji, rozdzielczości obrazu, liczby klatek/sek., okresu archiwizacji dla trybu imprezy masowej i trybu standardowego.
- Możliwość konfiguracji prędkości transmisji niezależnie dla każdej stacji klienckiej i każdego użytkownika, pozwalające na wyświetlanie obrazu z tej samej kamery z różnymi prędkościami dla różnych użytkowników.
- Multi streaming – wykorzystanie dowolnej ilości strumieni obrazowych generowanych przez kamerę w ramach jednej licencji kamerowej.
- Obsługa jedno i dwukierunkowej transmisji dźwięku.
- Tworzenie wirtualnych przycisków – umożliwiających sterowanie wyjściami w kamerach i zewnętrznych modułach I/O, oraz wywoływanie zdefiniowanych scenariuszy alarmowych
- Możliwość wykrywania ruchu w obrazie.
- Obsługa sprzętowej detekcji ruchu w kamerach.
- Obsługa modułów inteligentnej analizy obrazu zaimplementowanej w kamerach IP.
- Obsługa inteligentnej analizy obrazu zaimplementowanej w kamerach IP.

-
- Schematy makro służące do szczegółowego określenia w jaki sposób ma być sterowany system i jakiego rodzaju akcje powinny zostać uruchomione w przypadku określonych rodzajów zdarzeń.
 - Uruchamianie przez zdefiniowane makra jednoczesnego zapisu dowolnej ilości kamer w przypadku pojawienia się alarmu.
 - Obsługa sieciowych modułów I/O (wejść/wyjść) wykorzystywana do łatwej i szybkiej integracji alarmów pochodzących z innych systemów.
 - Monitorowanie wszystkich zdarzeń oraz akcji w systemie, takich jak: zmiany w konfiguracji serwera oraz kamer, potwierdzenia alarmów, aktywacja przycisków, itp. oraz ich zapis w dzienniku zdarzeń przyporządkowanym do określonego operatora.
 - System musi zapewniać automatyczne przełączenie strumieni audio-wideo na serwer zapasowy w przypadku uszkodzenia któregoś z serwerów podstawowych.
 - System musi umożliwiać obsługę na urządzeniach mobilnych z systemami Android oraz iOS w tym:
 - odtwarzanie obrazu „na żywo”,
 - odtwarzanie zarejestrowanego obrazu,
 - wyświetlanie informacji o zdarzeniach alarmowych,
 - umożliwiać wywoływanie reakcji alarmowych na serwerze oraz aplikacjach klienckich innych operatorów.
 - Mechanizm automatycznej dystrybucji poprawek oprogramowania dla aplikacji serwerowej i klienckiej przez administratora systemu za pomocą aplikacji serwerowej umożliwiającej automatyczną instalację aktualizacji w tym m.in.:
 - automatyczne pobieranie aktualizacji z serwera producenta oprogramowania
 - tworzenie grup urządzeń podlegających aktualizacjom
 - zdalny przegląd wersji zainstalowanych aktualizacji na wszystkich serwerach oraz stacjach klienckich
 - automatyczną dystrybucję aktualizacji do zdefiniowanej grupy urządzeń
 - ręczną dystrybucję aktualizacji do zdefiniowanej grupy urządzeń
 - zdalny restart aplikacji klienckiej z poziomu aplikacji serwerowej

Tryb pracy operatorskiej - na żywo.

- Tryb wielomonitorowy - obsługa min. 4 monitorów przez każdą aplikację kliencką.
- Równoległa wizualizacja dowolnej liczby kamer.
- Równoczesne wyświetlanie na jednym monitorze obrazu w podziale z kamer oraz aktywnych map obiektu.
- Funkcja ściany monitorów - możliwość zarządzania zdalnymi monitorami przez uprawnionego operatora, w tym:

- możliwość wyświetlenia układu kamer lub kamery na monitorach podłączonych do innych stacji klienckich oraz możliwość wizualizacji aktualnie wyświetlanego obrazu na stacji uprawnionego operatora,
 - zmiana wyświetlanych widoków na ekranach należących do zdefiniowanych ścian monitorów poprzez funkcję złap i upuść z widoku pełnoekranowego na żywo, z listy kamer, z siatki kamer, aktywnych map wideo.
- Zarządzanie autoryzacjami umożliwiające, dla każdego z użytkowników z osobna, przyporządkowywanie szczegółowych uprawnień dotyczących dostępu do wyświetlania obrazu z określonych kamer, eksportu zapisanego materiału, sterowania kamerami PTZ, przycisków wirtualnych aktywujących makra, dostępu do elementów ścian monitorów.
 - Wywołanie makr oraz sterowanie układami kamer oraz mapami na monitorach z poziomu przycisków funkcyjnych na zewnętrznym pulpicie sterującym.

Tryb archiwum:

- Obsługa zapisu dla trybu dziennego, nocnego oraz alarmowego (alarm wywołany z poziomu zintegrowanych systemów)
- Czas zapisu definiowany indywidualnie dla kamery lub grupy kamer, z rozróżnieniem zapisu normalnego oraz w trybie alarmu
- Rozrzadzanie zapisanego materiału wideo, dla materiału rejestrowanego w trybie dziennym, nocnym.
- Odtwarzanie obrazu z prędkością do 50x.
- Płynne odtwarzanie obrazu „do przodu” oraz „do tyłu”.
- Materiał eksportowany zabezpieczony hasłem.
- Jednoczesny eksport wszystkich lub wybranych kamer do jednego pliku.

- Automatyczny podział eksportowanego materiału na pliki o pojemności odpowiadającej pojemnościom płyt CD, DVD oraz Blu-ray.
- Zabezpieczenie zapisanego i oznaczonego materiału przed nadpisaniem na serwerach.
- Zapisywanie znaczników (tagi) w bazie danych oraz możliwość przeszukiwania archiwum po dowolnej części opisu znacznika.

6.1.5 Minimalne parametry dla stacji klienckich:

- Procesor ośmiordzeniowy osiągający wynik nie mniejszy niż 40.000 punktów w testach Passmark.
- Pamięć RAM: min. 32 GB DDR5, z możliwością rozbudowy do 128GB
- Podstawowy dysk twardy: o pojemności min. 480GB,
- Karta graficzna:
 - 4 monitorowa – pamięć min. 12GB
- Karta sieciowa 1000 Mbit/s
- Złącza min.:
 - 2 x USB 3 Type-A
 - 1 x USB 3 Type-C
 - 2 x USB 2
 - Uniwersalny port audio
 - RJ45 Ethernet port, 1GbE
 - DisplayPort 1.4
- System operacyjny 64 bitowy z obsługą „Active Directory” zgodny z wymogami producenta oprogramowania
- Zasilacz min. 500W o wydajności zapewniającej prawidłową pracę komputera wyposażonego w dedykowaną kartę graficzną
- 5 lat gwarancji
- Wyposażona w mysz oraz klawiaturę

6.1.6 Minimalne parametry dla stosowanych serwerów:

- serwer do montażu w szafie Rack obsługujący min. 4 dyski 2,5 lub 3,5" z kieszeniami „Hot swap” (pozwalającymi na wymianę dysków w trakcie pracy serwera).
- wysokość 1U
- system operacyjny zainstalowany na 2 dyskach SSD o pojemności min. 480GB skonfigurowanych w układzie RAID-1,
- procesor dziesięciordzeniowy osiągający wynik nie mniejszy niż 30.000 punktów w testach Passmark.
- możliwość instalacji 2 procesorów
- pamięć RAM min. 128 GB wyposażona w system kodowania korekcyjnego (ECC)
- min 2 interfejsy sieciowe LAN 1GbE
- min 2 interfejsy sieciowe LAN 10GbE
- kontroler sprzętowy RAID wspierający układ RAID-1,
- dostarczone dyski twarde dedykowane do pracy ciągłej w trybie 24 godziny 7 dni w tygodniu
- karata zarządzająca zapewniająca zdalne zarządzanie serwerem
- zasilacz redundantny 1+1 „hot plug”
- system operacyjny serwerowy 64-bitowy, zgodny z wymogami producenta oprogramowania rejestrującego oraz integrującego.
- 5 lat gwarancji

Całkowita pojemność przestrzeni dyskowej przeznaczona na archiwum musi zapewnić zapis 30 dni z zachowaniem pełnej jakości oraz prędkości strumieni wideo.

6.1.7 Minimalne parametry dla stosowanych macierzy:

- dla potrzeb systemu VSS, macierz należy wyposażać w dyski twarde, skonfigurowane w układzie RAID-5 + 1 dysk „Hot spare”
- dla potrzeb systemu integrującego macierz należy wyposażać w dwa syki SAS 2,4TB skonfigurowane w układzie RAID-1,

- wszystkie dostarczone dyski muszą być dedykowane do pracy ciągłej w trybie 24 godziny 7 dni w tygodniu

- kontroler RAID wspierający układy 0, 1, 5, 6, 10, 50; pamięć RAM kontrolera min. 8GB, szybkość transferu danych min. 12 Gbit/s.

- podwójny redundantny kontroler,
- montaż min. 2 kart interfejsów 4 x1Gb/s z możliwością wymiany w czasie pracy,
- porty SAS 12Gb,
- pamięć RAM min. 8GB,
- zasilacz redundantny min. 2 x 450 W,
- możliwość instalacji min. 12 dysków 2,5"/3,5",
- montaż w szafie Rack 19" za pomocą dedykowanych szyn montażowych,
- 5 lat gwarancji

6.1.8 Minimalne parametry dla stosowanych kamer tubowych:

- matryca wideo: 1/2,8" CMOS
- rozdzielczość: 3840 × 2160 pikseli (8 MP)
- prędkość: do 30 kl/s w pełnej rozdzielczości
- obiektyw: regulowany motozoom 2,7–13,5 mm
- światłoczułość: 0,005 lx / F1.6, 0 lx przy włączonym IR
- IR: zasięg do 60 m,
- kodowanie: H.265, H.264,
- wielostrumieniowość: 3 strumienie
- funkcje poprawy jakości obrazu: WDR 120 dB, 2D/3D DNR,
- obsługa protokołów i integracja: ONVIF Profile S/G/T,
- interfejs audio: wej./wyj. liniowe, obsługa 2-kierunkowego audio (full duplex)
- analityka: zliczanie osób, detekcja intruza, multi-loitering, smart motion detection (SMD), klasyczna detekcja ruchu, detekcja sabotażu
- zasilanie: 12 V DC, PoE

- wejścia/wyjścia alarmowe: 1 wejście / 1 wyjście
 - klasa szczelności: IP67
 - klasa odporności: IK10
 - temperatura pracy: od -40°C do +60°C
 - pobór mocy do 7,5 W
 - 5 lat gwarancji
- kamery należy wyposażyć w dedykowaną puszkę montażową

6.1.9 Minimalne parametry dla stosowanych kamer kopułowych:

- matryca wideo: 1/2,8" CMOS
- rozdzielczość: 2592 × 1944 pikseli (5 MP)
- prędkość: do 30 kl/s w pełnej rozdzielczości
- obiektyw: regulowany motozoom 2,7–13,5 mm
- światłoczułość: 0,005 lx / F1.6 (kolor, 30 IRE); 0 lx przy włączonym IR
- IR: zasięg do 50 m
- kodowanie: H.265 / H.264
- wielostrumieniowość: 3 strumienie
- funkcje poprawy jakości obrazu: WDR 120 dB, 2D/3D DNR
- obsługa kart SD
- obsługa protokołów i integracja: ONVIF (Profile G/S/T)
- interfejs audio: wej./wyj. liniowe, obsługa 2-kierunkowego audio (full duplex)
- analityka: zliczanie osób, detekcja intruza, multi-loitering, smart motion detection (SMD), klasyczna detekcja ruchu, detekcja sabotażu
- zasilanie: 12 V DC, PoE
- wejścia/wyjścia alarmowe: 1 wejście / 1 wyjście
- klasa szczelności: IP67
- klasa odporności: IK10
- temperatura pracy: od -40°C do +60°C
- pobór mocy do 6 W

- 5 lat gwarancji
- kamery należy wyposażyć w dedykowaną puszkę montażową.

6.1.10 Minimalne parametry dla stosowanych kamer obrotowych:

- matryca wideo: 1/2,8" CMOS
 - rozdzielczość: 2592 × 1944 pikseli (5 MP)
 - prędkość: do 30 kl/s w pełnej rozdzielczości
 - obiektyw: regulowany motozoom min 5,5 – 95 mm
 - światłoczułość: 0,007 lx / F1.6
 - IR: zasięg do 150 m
 - kodowanie: H.265 / H.264
 - wielostrumieniowość: 3 strumienie
 - funkcje poprawy jakości obrazu: WDR 120 dB, 2D/3D DNR
 - obsługa kart SD
 - obsługa protokołów i integracja: ONVIF (Profile M/G/S/T)
 - interfejs audio: wej./wyj. liniowe, obsługa 2-kierunkowego audio (full duplex)
 - analityka: detekcja ruchu, detekcja zmiany sceny, wykrycie intruza, detekcja szwędania się, zliczanie osób, detekcja przecięcia linii, detekcja twarzy,
 - zasilanie: 24 VAC, 36 VDC, PoE+
 - wejścia/wyjścia alarmowe: 2 wejście / 2 wyjście
 - klasa szczelności: IP66
 - klasa odporności: IK10
 - temperatura pracy: od -40°C do +60°C
 - pobór mocy do 25 W
 - 5 lat gwarancji
- kamery należy wyposażyć w dedykowany adapter montażowy.

6.1.11 Minimalne parametry dla stosowanych przełączników sieciowych:

- Przełącznik 24 portowy PoE warstwy 3

Parametry podstawowe:

- 24 porty Ethernet GEi 4 porty 10G SFP,

- 4 porty uplink 10G SFP+, 1

- Power over Ethernet (budżet PoE 370 W),
- Podstawowe funkcje warstwy 3
- Obsługa PoE zgodnie ze standardem IEEE 802.3af/at
- Bezpieczeństwo dzięki konfigurowalnej kontroli dostępu na wszystkich portach zgodnie ze standardem IEEE 802.1X
- Bezpieczne zdalne zarządzanie za pośrednictwem TACACS+, SSH, SSL i SNMPv3
- Przechowywanie i przekazywanie z opóźnieniem poniżej 4 mikrosekund
- Obsługa maks. 16 tys. adresów MAC
- Przepustowość: 65 Gb/s
- Maksymalne przetwarzanie pakietów 50 MPPS przy pakietach 64-bajtowych
- Sieć VLAN oparta na portach i znacznikach IEEE 802.1q z maksymalnie 4093 sieciami VLAN; Obsługuje filtrowanie pakietów przychodzących i wychodzących
- Obsługa ramek Jumbo z maksymalnie 10240 bajtami
- Funkcje warstwy 3
- Routing statyczny sprzętowy (IPv4/IPv6) z liczbą 128 możliwych tras
- Serwer DHCP na sieć VLAN, maks. 16 pul
- Protokół Tree Protokoll (STP) / Rapid STP / Multiple STP
- Protokół kontroli agregacji łączy (Link Aggregation Control Protocol) (LACP)
- Obsługa 26 grup zawierających do 4 portów każda zgodnie z IEEE 802.1ax
- Obsługa do 4 tys. sieci VLAN jednocześnie (z 4093 identyfikatorów VLAN); dopasowanie według portu, sieci VLAN oznaczonych IEEE 802.1q, adresów MAC, podsieci IP i funkcji Private VLAN Edge („chronione porty”)
- IGMP v1, v2, v3 w celu ograniczenia ruchu multicast wymagającego dużej przepustowości do portów z requesterami, 1024 grupy multicastowe;
- Serwer proxy IGMP do przesyłania komunikatów IGMP

- 5-letnia gwarancja

6.2 Opis integracji z systemami VSS, KD, SSWIN, SAP

Podstawowe zadania systemu integrującego:

Odbiór i rejestracja wszystkich informacji związanych z pracą integrowanych systemów,

Sortowanie i filtrowanie danych pod względem priorytetu raportowania i sposobu prezentacji informacji,

Mapowanie wybranych informacji na precyzyjnie zdefiniowane alarmy, zgodnie z wymaganiami użytkownika,

Komunikowanie zagrożeń użytkownikowi w maksymalnie czytelny sposób: w postaci tabliczek alarmowych ze wskazaniem lokalizacji na wektorowej mapie obiektu,

Zarządzanie podległymi systemami,

Automatyczne nadawanie komunikatu w relacji na zdarzenia raportowane przez integrowane systemy,

Uruchamianie automatycznych relacji pomiędzy integrowanymi systemami,

Umożliwia obsługę weryfikacji wizyjnej zdarzeń poprzez przypisanie obrazu kamery CCTV.

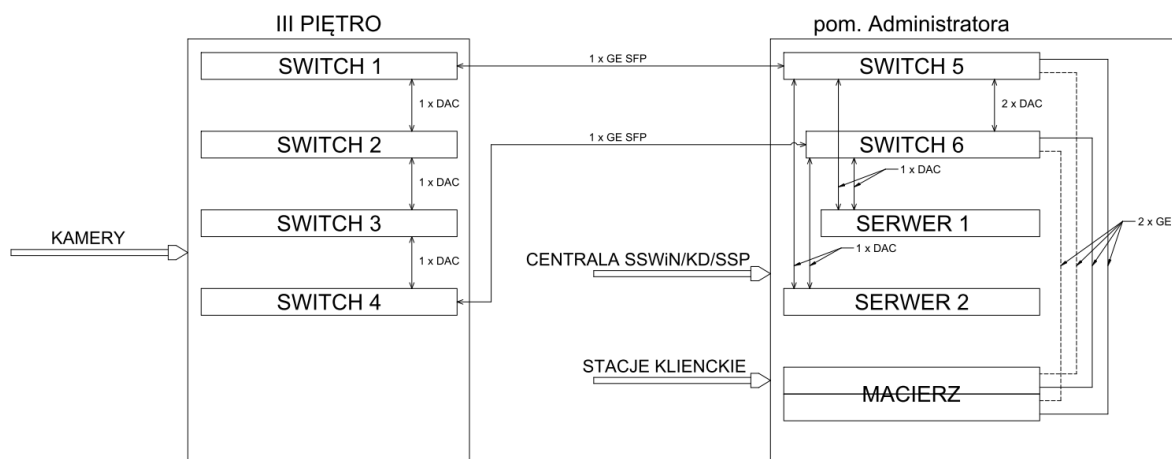
System integrujący musi obejmować co najmniej systemy:

Istniejący system sygnalizacji pożarowej,

Istniejący system sygnalizacji włamania i napadu,

Istniejący system kontroli dostępu

Nowo projektowany systemy monitoringu wizyjnego VSS



Prezentacja informacji:

Prezentacja informacji pochodzących od integrowanych systemów bezpieczeństwa jest realizowana w oparciu o ujednolicone tabliczki informacyjne prezentowane na głównym ekranie alarmowym. Taka prezentacja informacji znacznie skraca czas reakcji użytkownika. Tabliczki alarmowe są lokalizowane na ekranie w oparciu o kryteria związane z czasem wystąpienia alarmu oraz z poziomem priorytetu prezentowanej informacji.

System musi automatycznie i precyzyjnie wskazać operatorowi lokalizację zagrożenia. Elementy integrowanych systemów odwzorowane są w postaci interaktywnych ikon rozmieszczonych na wektorowych mapach obiektu. Każda ikona elementu, po wskazaniu kursorem, rozwija własne dynamiczne menu z wykazem poleceń dostępnych dla zalogowanego użytkownika.

Zakres informacji:

SYSTEM SYGNALIZACJI WŁAMANIA I NAPADU

- Prezentacja i logowanie zdarzeń/alarmów,
- Prezentacja aktualnych stanów linii i obszarów,
- Zarządzanie grupami alarmowymi i poszczególnymi liniami alarmowymi,

SYSTEM KONTROLI DOSTĘPU

- Prezentacja i logowanie zdarzeń/alarmów,
- Prezentacja aktualnych stanów przejść,
- Zarządzanie przejściami,
- Wydawanie kart dostępu z poziomu aplikacji klienckiej integratora

SYSTEM PRZYWOŁAWCZY I INTERKOM

- Odbieranie i nawiązywanie połączeń,
- Zwalnianie blokady przejścia,
- Prezentacja i logowanie zdarzeń/alarmów,
- Automatyczne wyzwalania komunikatów

MONITORING WIZYJNY CCTV

- Prezentacja alarmów na wspólnej mapie graficznej z uwzględnieniem alarmów naruszenia stref,
- Prezentacja i logowanie zdarzeń/alarmów,
- Przywołanie strumienia obrazu ze wskazanej kamery,
- Automatyczne przywołanie strumienia obrazu związanego ze zdarzeniem,
- Automatyczne umieszczanie adnotacji alarmowych w bazie danych VSS z opisem zdarzenia oraz oznaczeniem detektorów alarmowych
- Wywoływanie obrazu z bazy danych video VSS w trakcie weryfikacji alarmów zgodnie z czasem wystąpienia alarmu

SPECYFIKACJA SYSTEMU:

Cechy systemu integrującego:

- Wspólny interfejs składający się z mapy wektorowej i elementów interaktywnych dla wielu systemów – KD, CCTV, SSP itd.
- Podział obiektu na piętra czy regiony, możliwość nawigacji oraz płynnego przechodzenia,
- Zarządzanie udostępnionymi funkcjami integrowanych systemów oraz interakcje pomiędzy nimi,

- Nieorganiczna ilość profili użytkowników, do 64 operatorów pracujących jednocześnie w systemie,
- Magistrale komunikacyjne szyfrowane klucz 128bit,
- Szerokie kryteria raportowania – zarówno raporty predefiniowane jak i zewnętrzne;
- Zdarzenia i alarmy zapisywane w czasie rzeczywistym,
- Wielopoziomowe mapy graficzne do łatwiejszego lokalizowania miejsca alarmów, załączane również do okna dialogowego z alarmem,
- Dowolny nośnik do połączenia z centralami: RS232, RS485, LAN, WAN,
- Możliwość tworzenia back-upu danych oraz konfiguracja z serwerem zapasowym,
- Pełny rejestr zdarzeń zapisywany w bazie danych,
- Graficzna obsługa rejestru alarmowego,
- Dodatkowe informacje/ procedury dla obsługi przy przeglądaniu zdarzeń (okno podpowiedzi);

6.3 Opis bramki obrotowej

Podczas analizy stwierdzono konieczność wymiany bramek obrotowych w holu głównym budynku. Na etapie projektowania należy uzgodnić z Użytkownikiem dokładną lokalizację nowych bramek. W przypadku zmiany lokalizacji bramek należy uzgodnić projekt pod względem architektonicznych, wymaganiami dla osób niepełnosprawnych oraz pod kątem bezpieczeństwa PPOŻ (droga ewakuacji).

Urządzenia przeznaczone są do wspomagania kontroli ruchu osobowego w miejscach strzeżonych wewnątrz budynków. Bramki dedykowane jako punkty weryfikacji uprawnień wejścia oraz rejestracji czasu pracy.



Podstawowe parametry urządzeń:

Bramka wyposażona w podwójny system blokady zabezpieczający przed próbą przepchnięcia. Pierwszy poziom zabezpieczenia stanowi hamulec elektromagnetyczny, natomiast drugi – mechaniczny system blokady oparty na zespole zapadek sterowanych cewkami oraz na kole zębatym.

Bramka wyposażona jest również w sprzęgło kulkowe, które dostosowuje pracę mechanizmu do prędkości przejścia użytkownika, zapewniając płynne i komfortowe działanie.

Modułowa konstrukcja mechanizmu ułatwia serwisowanie urządzenia oraz szybką wymianę elementów uszkodzonych lub zużytych w wyniku długotrwałej eksploatacji. Silnik wspomagający obrót stanowi niezależny element mechanizmu i jest połączony z nim za pomocą paska zębatego.

Możliwość łatwej konfiguracji trybów działania i funkcji za pomocą panelu sterującego z wyświetlaczem i manipulatorem.

Sygnalizacja wizualna (piktogramy diodowe) informują o włączonych i wyłączonych z działania kierunkach możliwego ruchu w sekcji przejścia. Czerwony krzyżyk informuje o stanie

wyłączenia/zablokowania (urządzenie uniemożliwia przejście osoby) kierunku ruchu, zielona strzałka informuje o stanie odblokowania kierunku ruchu.

Urządzenie umożliwia pracę w różnych trybach np.: kontrola ruchu osobowego dla obu kierunków ruchu lub kontrola ruchu osobowego dla dowolnego wybranego kierunku ruchu.

Urządzenie jest wyposażone w elektroniczny układ pomiaru pozycji rotora umożliwiający układowi sterującemu sterowanie pracą systemu blokad oraz płynną szybkością ruchu ramion dla modelu z elektromechanicznym wspomaganie ruchu ramion.

Urządzenie wspomaga kontrolę ruchu osobowego w obu kierunkach, zarówno przy wejściu jak i wyjściu z chronionego obszaru.

Funkcja automatycznego opadania ramienia w przypadku zaniku napięcia.

Urządzenie posiada blokadę z układem amortyzującym, co znacząco wydłuża żywotność mechanizmu.

Mechanizm urządzenia wyposażony jest w elektromechaniczny układ wspomagający ruch obrotowy ramion. Układ ten po przyłożeniu siły na ramię rotora (pchnięciu) załącza silnik, który wspomaga obrót rotora do pozycji wyjściowej.

Urządzenie można połączyć z inteligentnym systemem zabezpieczeń w budynku.

7. Zagadnienia BHP, normy

- PN-EN 62676-1-1:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 1-1: Wymagania systemowe - Postanowienia ogólne,
- PN-EN 62676-1-2:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 1-2: Wymagania systemowe - Wymagania eksploatacyjne dotyczące transmisji wizji,
- PN-EN 62676-2-1:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 2-1: Protokoły transmisji wizji - Wymagania ogólne,
- PN-EN 62676-4:2015-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach - Część 4: Wytyczne stosowania,

Obowiązujące normy i wytyczne w zakresie budowy systemów sieci informatycznych w szczególności:

- PN-EN 50173-1,
- PN-EN 50174-1,
- PN-EN 50174-2,
- PN-EN 50174-3,
- PN-EN 50310,
- PN-EN 50346,
- PN-ISO/IEC 2382-25:1996,

UWAGA:

W przypadku powołań normatywnych niedatowanych obowiązuje zawsze najnowsze wydanie cytowanej normy.

8. Wytyczne dla Wykonawców

Projekt i montaż urządzeń powinien być wykonany przez Wykonawcę posiadającego wiedzę i doświadczenia w zakresie projektowania, montażu, konfiguracji i uruchamiania tego typu systemów.

Projektant musi posiadać odpowiednie uprawnienia budowlane i aktualny wpis do Izby Inżynierów Budownictwa.

Kierownik budowy musi posiadać odpowiednie uprawnienia budowlane i aktualny wpis do Izby Inżynierów Budownictwa.

Projekt musi zawierać wszelkie konieczne uzgodnienia.

Po wykonaniu projektu należy złożyć go Inwestorowi w celu zatwierdzenia.

Po wykonaniu robót budowlano montażowych należy dostarczyć gwarancję i instrukcję obsługi zainstalowanych urządzeń i oprogramowania oraz instrukcję postępowania w przypadku awarii.

Po uruchomieniu systemów należy przeszkolić osoby wskazane przez Inwestora z zakresu obsługi urządzeń oraz wykrywania podstawowych uszkodzeń.

Wykonawca może zastosować materiały, urządzenia i oprogramowanie o parametrach technicznych takich jak podano w niniejszym opracowaniu lub lepszych po uzgodnieniu z Inwestorem.

Wszystkie zastosowane materiały muszą posiadać stosowne atesty, świadectwa, certyfikaty, dopuszczające je do stosowania w budownictwie na terenie Rzeczypospolitej Polskiej. Dla każdego urządzenia aktywnego należy założyć paszport techniczny.

9. Kosztorys Inwestorski i przedmiar robót.

- Kosztorys inwestorski stanowi Załącznik nr 1 do niniejszej Dokumentacji Technicznej.
- Przedmiar robót stanowi Załącznik nr 2 do niniejszej Dokumentacji Technicznej.