ZATWIERDZAM
Wydziału Teleinformatyki
Komendy Stołecznej Policji
mł. insp. Mariusz GALARDA

Wytyczne Wydziału Teleinformatyki Komendy Stołecznej Policji do projektowania systemów i sieci w obiektach Komendy Stołecznej Policji

Wersja dokumentu 1.0

Warszawa, kwiecień 2022r.

Spis treści

Wstęp

W celu zapewnienia spełnienia zasadniczych wymagań technicznych i funkcjonalnych, projektowanie i budowa infrastruktury telekomunikacyjnej, teleinformatycznej oraz radiowych systemów stacjonarnych w obiektach przeznaczonych dla jednostek i komórek organizacyjnych Policji, odbywa się w porozumieniu i pod nadzorem Wydziału Teleinformatyki KSP.

Budowa systemów okablowania strukturalnego dla sieci komputerowej i łączności przewodowej oraz radiowych systemów stacjonarnych w obiektach siedzib jednostek Policji zapewnić musi spełnienie zasadniczych wymagań oraz spełniać zarówno unijne, jak i światowe standardy.

Wszystkie proponowane na etapie założeń projektowych oraz projektów branżowych wykonawczych rozwiązania oraz technologie powinny uzyskać pisemną akceptację Wydziału Teleinformatyki KSP.

Projekt Wykonawczy branży teletechnicznej należy podzielić na działy zgodnie z projektowanymi systemami teleinformatycznymi (LAN, SSWiN, SKD, CCTV IP i inne). Każdy z działów powinien zawierać osobny spis treści, opis, rysunki i schematy danego systemu.

Szczegółowe wymagania:

1. Na Serwerownie Główne oraz Lokalne Punkty Dystrybucyjne należy wyznaczać pomieszczenia znajdujące się na parterze lub wyżej. Podczas planowania należy pamiętać, że pomieszczenia te będą przeznaczone na cele techniczne, dlatego też należy zapewnić odpowiedni dostęp do kanalizacji technicznej obiektowej i publicznej.
2. Serwerownie i pomieszczenie dystrybucyjne powinno posiadać zabezpieczenia przed dostępem osób niepowołanych (System Kontroli Dostępu). Minimalne zabezpieczenie to książka wydawania kluczy oraz zamknięcie plombownicze (referentka) oraz okresowe kontrolowanie zgodności referentki z książką wydawania kluczy. Zalecany jest system kontroli dostępu oparty o użyte w KSP osobiste karty kontroli dostępu oraz zamontowanie alarmu (System Sygnalizacji Włamania i Napadu).
3. Pomieszczenie należy tak zaprojektować w budynku, aby odległość kablowa od najdalszego abonenta nie przekraczała 90 metrów. Jeżeli odległość ta będzie większa to należy zaprojektować więcej niż jedno pomieszczenie. Połączenia pomiędzy punktami dystrybucyjnymi należy wykonywać: kablem światłowodowym minimum 24 włókna SM oraz kablem wieloparowym miedzianym (min. 24 pary) oraz jeśli długość nie przekracza 90m połączenie LAN FTP Cat. 6 x24. Wszystkie połączenia powinny być zakończone na odpowiednich panelach krosowych o n/w standardach:
    - Zakończenie kabli światłowodowych standard SC/APC
    - Zakończenie struktury LAN, gniazda i patchpanel Cat. 6
    - Zakończenie kabli miedzianych, łączówka krone lub patchpanel (rodzaj rozwiązania uzgodnić z WTI KSP)
4. Serwerownia/GPD/LPD powinna być umieszczona w pomieszczeniu bez okien, jeśli nie ma takich możliwości technicznych to zastosowane szyby w otworach okiennych powinny posiadać klasę odporności P4 oraz antywłamaniowe okucia okienne. W oknach powinny być zamontowane żaluzje antywłamaniowe. Ponadto jeżeli okno jest narażone na bezpośrednie działanie promieni słonecznych przez większą część

dnia, w celu zapewnienia odpowiednich warunków klimatycznych pomieszczenia oraz ograniczyć koszty funkcjonowania zainstalowanego systemu klimatyzacji należy zastosować szyba o niskim współczynniku przegrzewania. Szyby w oknach powinny być zabezpieczone folią matową uniemożliwiająca podgląd zewnątrz osobom nieuprawnionym.

5. Wielkość pomieszczenia Serwerowni oraz GPD nie powinna być mniejsza niż 20 m^2 i zapewnić możliwość posadowienia wszystkich zaprojektowanych szaf dystrybucyjnych 19" 42U (800cmx1000cm) oraz jednej zapasowej. Pomieszczenie LPD powinno pomieścić co najmniej dwie szafy dystrybucyjne 19" 42U (800cmx1000cm). We wszystkich typach pomieszczeń należy również przewidzieć miejsce na jedną szafę biurową na przechowywanie elementów wyposażenia: kabli, dokumentacji, nośników danych elementów zasilania itp.). Maksymalne wymiary projektowanego pomieszczenia Serwerowni, GPD oraz LPD bezpośrednio uzależnione są od spełnianej funkcji technicznej i w związku z tym wymagana jest w każdym przypadku konsultacja oraz akceptacja WTI KSP.
6. Szafy dystrybucyjne powinny być odsunięte minimum 50cm od ścian tak by możliwe było zdjęcie ich osłon/drzwi. Dodatkowo front szafy musi znajdować się minimum 150 cm od ścian i innych urządzeń tak, by w przyszłości można było swobodnie wymienić lub dołożyć urządzenia sieciowe. Natomiast tył szafy powinien być w takiej odległości od ściany, aby możliwe było swobodne otwarcie drzwi tylnych. Szafy muszą być wyposażona w przewiewne (perforowane) drzwi (obieg powietrza), posiadać możliwość zamknięcia na klucz i zastosowania zamknięcia plombowniczego (tzw. referentki).
7. Szafy dystrybucyjne wewnętrzne należy wyposażyć w panele wentylacyjne, panele krosownicze kat. min. 6a z gniazdami RJ-45 oraz dwoma listwami zasilającymi po minimum 8 gniazd każda, z sygnalizacją optyczną napięcia z wyłącznikiem listwy.
8. Wymaga się, aby w w/w Punktach Dystrybucyjnych w pomieszczeniach technicznych stosować odpowiednie urządzenia klimatyzacyjne zapewniające poprawną pracę urządzeń aktywnych sieci zdolnych utrzymać temperaturę max. 20 stopni C przy uwzględnieniu wydzielanej ciepłoty urządzeń. Wybór miejsca montażu klimatyzatora musi zapewniać brak możliwości zalania bądź innego uszkodzenia struktury teleinformatycznej lub energetycznej.
9. Pomieszczenia powinny być wyposażone w technologiczną podłogę podniesioną lub wykładzinę antystatyczną.
10. Pomieszczenia dystrybucyjne muszą być przygotowane w sposób minimalizujący zagrożenie pożarowe - podłoga niepalna, w pomieszczeniu musi być zainstalowany system sygnalizacji przeciwpożarowej. Instalacja alarmowa pożaru powinna być wyposażona w czujki wczesnego ostrzegania (czujki wykrywania tlenku węgla, dymu itp.) Pomieszczenie serwerowni winno być wyposażone w system do gaszenia urządzeń pracujących pod napięciem (system gazowy). Wskazane jest stosowanie automatów gaśniczych.
11. Ciągi komunikacyjne i otwory drzwiowe nie powinny stanowić utrudnienia przy przemieszczaniu elementów serwerowni (drzwi minimum 100cm szerokości).
12. Wysokość pomieszczeń powinna być nie mniejsza niż 2,5 m.
13. Wytrzymałość stropu: min 1 tona / 1m^2.
14. Pomieszczenia Serwerowni, GPD oraz LPD należy wyposażyć w dedykowany system uziemienia w przedziale od 2 do 5 Ω.

15. Szafy dystrybucyjne, siłownia telekomunikacyjna oraz inne urządzenia teletechniczne powinny być uziemione w sposób zapewniający poprawną pracę instalacji elektrycznej.
16. W pomieszczeniu serwerowni/GPD/LPD nie może być instalacji wodno-kanalizacyjnych, centralnego ogrzewania, gazowych. Instalacje te powinny być w takiej odległości od punktu dystrybucyjnego, aby nie stanowiły zagrożenia w przypadku ewentualnej ich awarii.
17. Pomieszczenia serwerowni/GPD/LPD nie mogą znajdować się bezpośrednio pod pomieszczeniami sanitarnymi.
18. Okablowanie teletechniczne należy prowadzić w korytach lub drabinkach kablowych. Okablowanie pionowe w korytach ściennych a poziome w przysufitowych drabinkach kablowych.
19. Okablowanie do szaf powinno być doprowadzane kanałami podpodłogowymi (jeżeli jest podłoga techniczna) lub od góry drabinkami kablowymi zamontowanymi bezpośrednio nad szafami.
20. Przepusty kablowe w ścianach należy uszczelniać specjalistyczną masą niepalną zgodnie z wymaganiami p-poż.

Zasilanie

1. Do pomieszczeń Serwerowni, Głównego oraz Lokalnego Punktu Dystrybucyjnego należy doprowadzić dedykowaną linię zasilającą z głównej tablicy obiektowej. Linię w serwerowni zakończyć tablicą rozdzielczą.
2. Tablica ta będzie zasilać wyłącznie urządzenia teleinformatyczne znajdujące się w pomieszczeniu (szafy serwerowe i siłownię telekomunikacyjną).
3. W przypadku braku w obiekcie zasilania gwarantowanego agregatem prądotwórczym i UPS-em należy wykonać z tablicy dodatkową linię zasilająca wyprowadzoną na zewnątrz budynku przeznaczoną do podłączenia zewnętrznego agregatu prądotwórczego. W takim przypadku niezbędnym jest zastosowanie ręcznego układu przełączenia zewnętrznego źródłu zasilania.
4. Elektryczna rozdzielnia obiektowa i urządzenia zasilania obiektowego (agregat i UPS) musi się znajdować poza pomieszczeniem serwerowni.
5. W Pomieszczeniach Serwerowni, Głównego oraz Lokalnego Punktu Dystrybucyjnego należy projektować Siłownię Telekomunikacyjną prądu przemiennego 230V i stałego 48V maksymalnie 8kVA z gwarantowanym podtrzymaniem minimum 6 godzin.
6. Panel dystrybucyjny siłowni należy zamontować w pierwszej szafie dystrybucyjnej.
7. Do każdej z pozostałych szaf doprowadzić obwód zasilania z siłowni telekomunikacyjnej.
8. Minimalne parametry zasilania na szafę 2x16A, zasilanie gwarantowane, wtyczki umieszczone przy podłodze szafy.
9. Każdą szafę dystrybucyjną należy wyposażyć w automatyczny przełącznik zasilania (dwa wejścia zasilania do jednego wyjścia), pozwalający na bezprzerwowe (czas przełączenia max 10ms) przełączanie zasilania pomiędzy źródłami zasilania (redundancja zasilania). Przełącznik ten musi posiadać zarządzanie przez sieć ethernetową oraz możliwość ręcznego wyboru źródła zasilania.
10. Wszystkie szafy muszą być podłączone do instalacji uziemiającej. W serwerowni musi być zamontowana szyna uziemiająca umożliwiająca podpięcie kolejnych szaf i urządzeń.

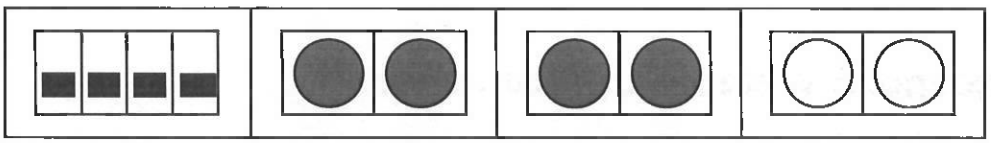
11. Jeżeli w jednostce jest planowane więcej punktów dystrybucyjnych to do każdego z nich powinno być doprowadzone zasilanie z siłowni telekomunikacyjnej, albo w każdym z nich zainstalowane siłownie telekomunikacyjne o odpowiednio dobranych parametrach obciążenia. Wszystkie punkty dystrybucyjne powinny być zasilane redundantnie z zasilania obiektowego gwarantowanego.
12. Zapewnienie zasilania gwarantowanego obiektowego dla pomieszczenia kierownika jednostki i sekretariatu, jak również stanowiska dowodzenia jednostki (Dyżurny i radio operator).
    - W przypadku, gdy jednostka posiada zestaw rezerwowego energetycznego zasilania bezprzerwowego (obiektowy UPS i agregat) linia zasilania gwarantowanego powinna ww. pomieszczenia powinny być wyposażone całościowo w gniazda zasilania obiektowego gwarantowanego UPS-em.
    - W przypadku, gdy jednostka nie posiada zestaw rezerwowego energetycznego zasilania bezprzerwowego (obiektowy UPS i agregat) linia zasilania gwarantowanego powinna być doprowadzona bezpośrednio siłowni telekomunikacyjnej i zakończone w ww. pomieszczeniach dedykowanymi gniazdami.

Okablowanie strukturalne LAN

1. Okablowanie strukturalne sieci LAN jednostek Policji musi być budowane w oparciu o aktualne normy ISO/IEC 11801:2002 (wersja ostateczna), ANSI EIA/TIA 568 B.2 (wersja ostateczna), EN 50173 oraz PN-EN 70153:2004. Budowę okablowania należy opierać o kable skrętkowe miedziane kategorii min. 6a ekranowane lub wyższej oraz o kable światłowodowe jednomodowe min 12-to włóknowe,
2. Nowo budowane okablowanie strukturalne należy wykonywać w standardzie kategorii min. 6 channel, poświadczone certyfikatem producenta,
3. Główne i Lokalne Punkty Dystrybucyjne należy wykonywać w pomieszczeniach technicznych, przeznaczonych na potrzeby urządzeń łączności i informatyki, w postaci szafy dystrybucyjnej z panelami krosowniczymi kat. min. 6a z gniazdami RJ-45 oraz dwoma listwami zasilającymi po minimum 8 gniazd każda, z sygnalizacją optyczną napięcia z wyłącznikiem listwy i opcjonalnym systemem wentylacji,
4. Pomieszczenia Serwerowni, GPD oraz LPD należy wyposażyć w dedykowany system uziemienia w przedziale od 2 do 5 Ω,
5. Szafa dystrybucyjna powinna być uziemiona w sposób zapewniający poprawną pracę instalacji elektrycznej,
6. Szafy dystrybucyjne powinny być odsunięte minimum 50cm od ścian tak by możliwe było zdjęcie ich osłon/drzwi. Dodatkowo przednie drzwi muszą znajdować się minimum 150 cm od ścian i innych urządzeń tak, by w przyszłości można było swobodnie wymienić lub dołożyć urządzenia sieciowe,
7. W przypadku konieczności połączenia dwóch punktów dystrybucyjnych (w dwóch budynkach) połączenie należy wykonywać kablem światłowodowym jednomodowym minimum 12 włóknowym zewnętrznym. Każde włókno należy zakończyć złączem SC/APC na panelu w szafie dystrybucyjnej,
8. Wymaga się, aby w przypadku zastosowania więcej niż jednego punktu dystrybucyjnego (w jednym budynku) okablowanie pionowe wykonać kablem światłowodowym jednomodowym minimum 12 włóknowym wewnętrznym. Każde włókno należy zakończyć złączem SC/APC na panelu w szafie dystrybucyjnej,

9. Wymaga się, aby system okablowania w szafie dystrybucyjnej składał się z 24 lub 48 portowych paneli, z gniazdami RJ45,
10. Oznaczenie gniazd powinno być spójne (przynajmniej dla całego obiektu) i jednoznacznie je identyfikujące,
11. Stosowane komponenty powinny pochodzić od jednego producenta oraz posiadać odpowiednie poświadczenie dopuszczenia do danej kategorii,
12. Wymaga się stosowanie szaf dystrybucyjnych o konstrukcji zgodnej do zastosowanego w pomieszczeniu systemu klimatyzacji,
13. Szafa dystrybucyjna powinna posiadać odpowiednie dedykowane do danego typu produktu: organizery kabli i uchwyty kablowe zapewniające uporządkowanie i zarządzanie kablami,
14. Wymaga się, aby całość oferowanej instalacji okablowania strukturalnego dla wskazanych lokalizacji miała możliwość dalszej rozbudowy w części logicznej: posiadać przekroje tras kablowych o 50% większą oraz wielkość szafy dystrybucyjnej dostosowane do zwiększenia struktury o 25%,
15. Przewody struktury LAN między poziomami powinny być puszczone PESZLEM (może być w rurach PCV) z możliwością powiększenia infrastruktury o 50%, na korytarzach w korytkach z możliwością powiększenia infrastruktury o 50%, (dopuszcza się korytka plastikowe) natomiast przewody biegnące wzdłuż sufitów podwieszanych powinny być umieszczone w korytkach perforowanych-aluminiowych z możliwością powiększenia infrastruktury o 50%, a w przypadku braku sufitów podwieszanych w korytkach z możliwością powiększenia infrastruktury o 50%,
16. Wymaga się, aby w Głównych i Lokalnych Punktach Dystrybucyjnych w pomieszczeniach technicznych stosować odpowiednie urządzenia klimatyzacyjne zapewniające poprawną pracę urządzeń aktywnych sieci,
17. Klimatyzatory **NIE MOGĄ** znajdować się nad urządzeniami elektrycznymi/ elektronicznymi w tym również włącznikami prądu, gniazdami sieciowymi itp.
18. Wymaga się, aby w trakcie budowy lub modernizacji systemów okablowań strukturalnych dokonywać integracji z istniejącą siecią telefoniczną,
19. Gwarancja producenta na okablowanie powinna wynosić min. 20 lat,
20. Pomiary połączenia powinny być wykonane metodą Permanent Link za pomocą mierników dla danej kategorii kabla i posiadających aktualną kalibrację,
21. Dokumentacja powykonawcza powinna zawierać przynajmniej: informacje ogólne, normy i zalecenia techniczne, ogólną strukturę okablowania, okablowanie pionowe, okablowanie poziome, opis instalacji zasilającej - gdy wchodzi w skład projektu, punkty dystrybucyjne, testowanie systemu, opis sposobu oznaczania przebiegów poziomych, specyfikacje materiałową oraz certyfikat zastosowanych komponentów, rysunki i schematy, wyniki pomiaru sieci, informację na temat posiadanych przez pracowników świadczących usługę uprawnień, kalibrację miernika, jak również dane na temat udzielanej gwarancji,
22. Okablowanie strukturalne powinno być zakończone w pomieszczeniu **punktem PEL 4xRJ45 i 2x230V gwarantowane i 2x230V normalne**,

PEL



23. Liczba PEL-i w danym pomieszczeniu powinna być określana na etapie projektowania sieci LAN w uzgodnieniu z użytkownikami końcowymi i Wydziałem Teleinformatyki KSP,

24. Wymaga się aby w miarę możliwości projektowych, w serwerowniach projektować podłogę teletechniczną zgodnie z obowiązującymi standardami, w przypadku braku możliwości wykonania podłogi teletechnicznej w pomieszczeniach takich jak serwerownia lub lokalny punkt dystrybucyjny, należy zastosować wykładzinę antyelektrostatyczną,

Wymaga się aby w miarę możliwości budowlanych, projektować na korytarzach wnęki dla urządzeń wielofunkcyjnych.

Pomieszczenia Serwerowni

Pomieszczenia łączności, informatyki, GPD (Główny Punkt Dystrybucji sieci logicznej), LPD (Lokalny Punkt Dystrybucji sieci logicznej):

1. Pomieszczenia centrali telefonicznej,
2. Pomieszczenia Serwerowni, GPD, LPD oraz urządzeń okresowego podtrzymania napięcia typu UPS,
3. Pomieszczenia łączności radiowej,
4. Pomieszczenia administratora sieci komputerowej.

Należy dążyć do zaprojektowania w obiekcie jednego pomieszczenia technicznego na cele łączności i informatyki o powierzchni użytkowej 20-25m2 (serwerownia) – w kształcie prostokąta o boku krótszym posiadającym wymiar nie mniejszy niż 3,0 m, w którym powinien znajdować się również centralny punkt dystrybucji (GPD). Wielkość pomieszczenia serwerowni powinna umożliwiać postawienie w przyszłości dodatkowej szafy dystrybucyjnej. Pomieszczenie to powinno być usytuowane w centralnej części budynku na parterze (w uzasadnionych przypadkach na piętrze) w strefie zamkniętej, obok pomieszczenia dyżurnego jednostki.

Z uwagi na ograniczenia techniczne, rozmieszczenie punktów dystrybucyjnych musi być takie, aby długości przewodów logicznych rozciąganych z tych punktów nie były dłuższe, niż 90 m. W serwerowni powinny znajdować się takie urządzenia jak: serwery, centrale telefoniczne, urządzenia sieciowe. Powinny one być wyposażone w system klimatyzacji precyzyjnej utrzymującą stałą temperaturę i wilgotność powietrza, zasilania gwarantowanego, system ppoż. Zaleca się również, zaprojektować podłogę techniczną umożliwiającą dostęp do instalacji IT i do instalacji zasilającej węzeł. Obudowa pomieszczenia i drzwi muszą spełniać wymogi określone dla pomieszczeń o wzmocnionej ochronie, wykładzina podłogowa powinna mieć właściwości antyelektrostatyczne. Oświetlenie naturalne w tych pomieszczeniach nie jest wymagane, zaś w przypadku występowania w nich okien muszą zostać spełnione wymagania jak dla pomieszczeń wzmocnionej ochrony.

Pomieszczenia administratora sieci komputerowej powinny spełniać wymagania jak dla pomieszczeń biurowych.

Łączność w sieciach radiowych

Dla realizacji łączności w sieciach radiowych Policji, na potrzeby stanowisk kierowania KSP/KPP/KRP, koniecznym jest uwzględnienie w projektowanych lub modernizowanych obiektach Policji infrastruktury dla radiokomunikacyjnych urządzeń stacjonarnych.

Wymagane jest wyposażenie projektowanego budynku w odpowiedni maszt antenowy, posadowiony na jego dachu lub wybudowanie w jego bezpośrednim sąsiedztwie, wolnostojącej wieży strunobetonowej (jako nośnika instalacji antenowej).

W budynku, w pobliżu masztu antenowego, należy przewidzieć odpowiednie pomieszczenie techniczne dla zainstalowania urządzeń radiokomunikacyjnych (radiotelefonów). Pomieszczenie to powinno zostać wyposażone w instalacje zasilającą oraz niezbędne okablowanie strukturalne dla potrzeb zdalnego sterowania radiotelefonów oraz klimatyzację.

Przyjęcie danego rozwiązania dotyczącego masztu antenowego, powinno brać pod uwagę lokalne uwarunkowania odnoszące się do propagacji fal radiowych, w tym położenie budynku oraz ukształtowanie terenu na obszarze działania danej jednostki, powinno zmierzać do zapewnienia wymaganego pokrycia zasięgiem radiowym obszaru działania jednostki Policji.

Powyższe rozwiązanie powinno być każdorazowo opracowane przez projektanta w uzgodnieniu ze Wydziałem Teleinformatyki KSP. **Wysokość masztu wieży należy każdorazowo uzgadniać z Wydziałem Teleinformatyki Komendy Stołecznej Policji.**

Maszty antenowe i pozostałe elementy infrastruktury radiokomunikacyjnej (anteny, przewody antenowe itp.) muszą zostać wyposażone w odpowiednią ochronę odgromową, zgodnie z obowiązującymi w tym zakresie normami oraz przepisami.

Kable antenowe na zewnątrz budynków powinny być prowadzone na wspornikach, natomiast wewnątrz z wykorzystaniem dedykowanych tuneli dla kabli antenowych do wszystkich pomieszczeń , w których zainstalowane są radiotelefony z zachowaniem rezerwy 30%.

Wszędzie tam gdzie pozwalają warunki przestrzenne preferowana jest budowa masztu strunobetonowego o wysokości minimum 40m z zainstalowaną iglicą odgromową zainstalowaną na szczycie masztu.

Jednocześnie ze względu na charakterystykę danej jednostki każdorazowo przed przystąpieniem do prac koncepcyjnych należy zweryfikować potrzeby jednostki.

Maszt/wieża ma być wyposażony w:

1. Drabinkę kablową,
2. Drabinkę systemową z system ochrony przeciw upadkowi SOLL (szyna asekuracyjna) z dwoma "wózkami" zgodnym z zastosowanym systemem asekuracji,
3. Dwa podesty techniczne z kratami pomostowymi oraz dodatkowy pierścień ponad górnym podestem technicznym. Oba pomosty oraz dodatkowy pierścień ponad górnym podestem technicznym połączone ze sobą pionowymi 3 belkami do których będą mocowane anteny radioliniowe, VHF, UHF (w przypadku wieży strunobetonowej),
4. Odpowiednią ilość poziomów odciągów dla konstrukcji rurowej lub kratowej,
5. Poręcze asekuracyjne.

Ze względu na przeznaczenie nowo projektowanego obiektu należy wyróżnić dwa rodzaje inwestycji różniących się ilością zainstalowanych środków radiowych. Dodatkowo należy wyróżniać dwa rodzaje zastosowanych konstrukcji wsporczych – maszt kratowy zainstalowany na dachu budynku, lub wolnostojącą wieżę strunobetonową.

I. Komenda Powiatowa / Rejonowa

1. Maszt ma być wyposażony w:
   a) 2 szt. Anten Procom CXL 2-5SL pracujące w paśmie 164-174MHz (lub równoważne) zainstalowane na szczycie masztu (na podeście technicznym w stożku ochronnym iglicy odgromowej),

b) 1 szt. anteny VHF Amphenol Procom CXL 2-3C-PT w wykonaniu „lightning protected" Anteny umieszczone na szczycie masztu (w stożku ochronnym iglicy odgromowej) z zachowaniem separacji pionowej minimum 1m od anten VHF Amphenol Procom CXL 2-5SL (Jako separację pionową należy rozumieć odstęp pomiędzy dolnym końcem wyższej anteny a górnym końcem anteny niższej,

c) 3 szt. anteny Radmor 32812 wyk.1 (pasmo pracy 146-174MHz) lub Amphenol Procom CXL2-1LW/h (pasmo pracy 156-174MHz) Rodzaj zastosowanej anteny zależy od lokalizacji i warunków propagacyjnych dlatego należy każdorazowo konsultować z WTI. Minimalna wysokość posadowienia najniższej anteny 15 m n.p.t. następne anteny montować z zachowaniem separacji pionowej pomiędzy antenami min. 1 m. Jako separację pionową należy rozumieć odstęp pomiędzy dolnym końcem wyższej anteny a górnym końcem anteny niższej,

d) 4 szt. anten UHF minimalny zakres pracy 380-395 MHz (Amphenol Procom CXL70-1LW/I – lub Amphenol Procom CXL70-3LW/I. Rodzaj zastosowanej anteny zależy od lokalizacji i warunków propagacyjnych dlatego należy każdorazowo konsultować z WTI.) wysokość posadowienia u szczytu masztu (odstęp 1m w pionie pomiędzy antenami. Rozmieszczenie w poziomie co 90 stopni, Anteny umieszczone na tym samym poziomie w pionie z odstępem 180 stopni w poziomie

e) 1 – 2 szt. anten radioliniowych wraz z modułami nadawczymi (w zależności od lokalizacji)

2. Pomieszczenie radiowe wyposażyć (w przypadku instalacji masztu antenowego na dachu budynku) :

a) Łącze światłowodowe 12J pomiędzy pomieszczeniem łączności a GPD (Główny Punkt Dystrybucji sieci logicznej), oraz 10 łączy RJ45 w relacji pomieszczeniem łączności a najbliższym LPD (Lokalny Punkt Dystrybucji sieci logicznej)

b) szafę RACK wewnętrzną wyposażoną w przednie i tylne drzwi perforowane, panel dystrybucji zasilania, oraz organizery kabli;

c) W szafie RACK należy zainstalować:
- zdalne sterowanie firmy TRX (SGM5ES) – 8 kpl.,
- radiotelefon MOTOROLA MTM5400 (TETRA) – 4 szt.,
- radiotelefon MOTOROLA DM4601e – 4 szt.

Dodatkowo należy wyposażyć system w:
- konsole dyspozytorskie wraz z ekranem dotykowym minimum 20 cali – 2 kpl.,
- manipulator wraz z serwerem klienckim (SGM5E) – 8 szt. w tym:
  - manipulator do radiotelefonów MOTOROLA MTM5400 (TETRA) – 4 szt.,
  - manipulator MOTOROLA DM4601e – 4 szt.

Manipulatory i konsole będą montowane na terenie budynku komendy.

d) W szafie RACK zainstalować stację retransmisyjną **RBS4000 Leonardo** lub równoważną i kompatybilną z systemem firmy LEONARDO SIMULCAST DMR.

3. W przypadku wykonania wolnostojącej wieży strunobetonowej u podstawy masztu zainstalować szafę RACK zewnętrzną z klimatyzacją.

a) Wybudować Łącze światłowodowe 12J pomiędzy pomieszczeniem łączności a GPD (Główny Punkt Dystrybucji sieci logicznej. Połączenie należy wykonywać kablem światłowodowym jednomodowym minimum 12 włóknowym zewnętrznym. Każde włókno należy zakończyć złączem SC/APC na panelu w szafie dystrybucyjnej.

b) Wykonać 2 przyłącza energetyczne do szafy RACK zewnętrznej:
- **Przyłącze Pierwsze**: przeznaczone do zasilania klimatyzatora i oświetlenia w szafie telekomunikacyjnej przy maszcie oraz urządzeń zainstalowanych w szafie - zasilanie gwarantowane w przypadku zaniku sieci zewnętrznej 230V agregatem,
- **Przyłącze Drugie**: przeznaczone do zasilania urządzeń telekomunikacyjnych w szafie telekomunikacyjnej przy maszcie - zasilanie gwarantowane w przypadku zaniku sieci zewnętrznej 230V agregatem i UPS obiektowym

c) szafę RACK zewnętrzną wyposażyć w klimatyzację;
d) W szafie RACK należy zainstalować:
- zdalne sterowanie firmy TRX (SGM5ES) – 8 kpl.,
- radiotelefon MOTOROLA MTM5400 (TETRA) – 4 szt.,
- radiotelefon MOTOROLA DM4601e – 4 szt.

Dodatkowo należy wyposażyć system w:
- konsole dyspozytorskie wraz z ekranem dotykowym minimum 20 cali – 2 kpl.,
- manipulator wraz z serwerem klienckim (SGM5E) – 8 szt, w tym:
  - manipulator do radiotelefonów MOTOROLA MTM5400 (TETRA) – 4 szt.,
  - manipulator do radiotelefonu MOTOROLA DM4601e – 4 szt.

  Manipulatory i konsole będą montowane na terenie budynku jednostki Policji.

e) W szafie RACK zainstalować stację retransmisyjną **RBS4000 Leonardo** lub równoważną i kompatybilną z systemem firmy LEONARDO SIMULCAST DMR.

II. Komisariat/Posterunek Policji podległy Komendzie Powiatowej/Rejonowej

1. Maszt ma być wyposażony w:
   a) 2 szt. Anten Procom CXL 2-5SL pracujące w paśmie 164-174MHz (lub równoważne) zainstalowane na szczycie masztu (na podeście technicznym w stożku ochronnym iglicy odgromowej),
   b) 1 szt. anteny Radmor 32812 wyk.1 (pasmo pracy 146-174MHz) lub Amphenol Procom CXL2-1LW/h (pasmo pracy 156-174MHz) Rodzaj zastosowanej anteny zależy od lokalizacji i warunków propagacyjnych dlatego należy każdorazowo konsultować z WTI.. Minimalna wysokość posadowienia najniższej anteny 15 m n.p.t. następne anteny montować z zachowaniem separacji pionowej pomiędzy antenami min. 1 m. Jako separację pionową należy rozumieć odstęp pomiędzy dolnym końcem wyższej anteny a górnym końcem anteny niższej,
   c) 1 szt. anten UHF minimalny zakres pracy 380-395 MHz (Amphenol Procom CXL70-1LW/I – lub Amphenol Procom CXL70-3LW/I lub równoważne. Rodzaj zastosowanej anteny zależy od lokalizacji i warunków propagacyjnych dlatego należy każdorazowo konsultować z WTI. Wysokość posadowienia u szczytu masztu (odstęp 1m w pionie pomiędzy antenami. Rozmieszczenie w poziomie co 90 stopni, Anteny umieszczone na tym samym poziomie w pionie z odstępem 180 stopni w poziomie,
   d) 1 – 2 szt. anten radioliniowych (w zależności od lokalizacji),

4. Pomieszczenie radiowe wyposażyć (w przypadku instalacji masztu antenowego na dachu budynku) :

   e) Łącze światłowodowe 12J pomiędzy pomieszczeniem łączności a GPD (Główny Punkt Dystrybucji sieci logicznej), oraz 10 łączy RJ45 w relacji pomieszczeniem łączności a najbliższym LPD (Lokalny Punkt Dystrybucji sieci logicznej)

f) szafę RACK wewnętrzną wyposażoną w przednie i tylne drzwi perforowane, panel dystrybucji zasilania, oraz organizery kabli;

g) W szafie RACK należy zainstalować:
   - zdalne sterowanie firmy TRX (SGM5ES) – 2 kpl.,
   - radiotelefon MOTOROLA MTM5400 (TETRA) – 1 szt.,
   - radiotelefon MOTOROLA DM4601e – 1 szt.

   Dodatkowo należy wyposażyć system w:
   - manipulator wraz z serwerem klienckim (SGM5E) – 2 szt, w tym:
     - manipulator do radiotelefonów MOTOROLA MTM5400 (TETRA) – 1 szt.,
     - manipulator MOTOROLA DM4601e – 1 szt.

     Manipulatory i konsole będą montowane na terenie budynku jednostki Policji.

h) W szafie RACK zainstalować stację retransmisyjną **RBS4000 Leonardo** lub równoważną i kompatybilną z systemem firmy LEONARDO SIMULCAST DMR.

5. W przypadku wykonania wolnostojącej wieży strunobetonowej u jej podstawy zainstalować szafę RACK zewnętrzną z klimatyzacją oraz systemem monitorowania stanu (Komenda Stołeczna posiada system nadzoru nad szafami AKCP)

f) Wybudować Łącze światłowodowe 12J pomiędzy pomieszczeniem łączności a GPD (Główny Punkt Dystrybucji sieci logicznej. Połączenie należy wykonywać kablem światłowodowym jednomodowym minimum 12 włóknowym zewnętrznym. Każde włókno należy zakończyć złączem SC/APC na panelu w szafie dystrybucyjnej.

g) Wykonać 2 przyłącza energetyczne do szafy RACK zewnętrznej:
   - **Przyłącze Pierwsze**: przeznaczone do zasilania klimatyzatora i oświetlenia w szafie telekomunikacyjnej przy maszcie oraz urządzeń zainstalowanych w szafie - zasilanie gwarantowane w przypadku zaniku sieci zewnętrznej 230V agregatem,
   - **Przyłącze Drugie**: przeznaczone do zasilania urządzeń telekomunikacyjnych w szafie telekomunikacyjnej przy wieży - zasilanie gwarantowane w przypadku zaniku sieci zewnętrznej 230V agregatem i UPS obiektowym

h) szafę RACK zewnętrzną wyposażyć w klimatyzację;

i) szafę RACK zewnętrzną wyposażyć w system monitorowania stanu (temperatury, zaniku zasilania, otwarcia drzwi) KSP posiada system nadzoru firmy AKCP;

j) W szafie RACK należy zainstalować:
   - zdalne sterowanie firmy TRX (SGM5ES) – 2 kpl.,
   - radiotelefon MOTOROLA MTM5400 (TETRA) – 1 szt.,
   - radiotelefon MOTOROLA DM4601e – 1 szt.

   Dodatkowo należy wyposażyć system w:
   - manipulator wraz z serwerem klienckim (SGM5E) – 2 szt, w tym:
     - manipulator do radiotelefonów MOTOROLA MTM5400 (TETRA) – 1 szt.,
     - manipulator MOTOROLA DM4601e – 1 szt.

     Manipulatory i konsole będą montowane na terenie budynku komendy.

k) W szafie RACK zainstalować stację retransmisyjną **RBS4000 Leonardo** lub równoważną i kompatybilną współpracującą z systemem firmy LEONARDO SIMULCAST DMR.

l) W szafie RACK zainstalować terminal radioliniowy INTRACOM TELECOM lub równoważny współpracujący z systemem zarządzania i nadzoru nad systemem radioliniowym UniMS firmy Intracom Telecom.

Ujednolicona Platforma Bezpieczeństwa – CCTV, SKD

W celu ograniczenia dostępu do niektórych obszarów w obiektach i pomieszczeniach służbowych osobom postronnym oraz w celu wyeliminowania zagrożeń przewiduje się instalację ujednoliconej platformy bezpieczeństwa (system kontroli dostępu SKD, monitoring wizyjny CCTV).

Wymagane minimalne parametry funkcjonalne i sprzętowe dla ujednoliconej platformy bezpieczeństwa z podsystemem KD wraz Wideodomofonem oraz podsystemu CCTV – *Genetec Security Center*

1.1 Planowany system monitoringu wizyjnego CCTV oraz kontroli dostępu KD musi wspierać bezproblemową integrację z istniejącą Platformą Bezpieczeństwa Komendy Stołecznej Policji *Genetec Security Center v.5.9*

1.2 Systemu kontroli dostępu IP (SKD) oraz systemu zarządzania monitoringiem CCTV IP (VMS) muszą być w jednej platformie.

1.3 Aplikacja interfejsu użytkownika (UI) będzie prezentować zunifikowany interfejs zabezpieczeń do zarządzania, konfiguracji, monitorowania i raportowania osadzonych systemów CCTV i SKD oraz powiązanych urządzeń brzegowych.

1.4 Funkcjonalności dostępne w ujednoliconej platformie bezpieczeństwa SSK KSP będą zawierać:

- Konfigurację osadzonych systemów takich jak CCTV, SKD, SSWiN.
- Monitorowanie zdarzeń na żywo.
- Monitorowanie wideo na żywo i odtwarzanie zarchiwizowanych nagrań.
- Zarządzanie alarmami.
- Raportowanie, jak również tworzenie własnych szablonów raportów i zdarzeń
- Możliwość federacji do istniejącego globalnego centrum monitorowania, raportowania i zarządzania alarmami zlokalizowanym w KSP w oparciu o protokół TCP/IP.
- Możliwość integracji z Microsoft Active Directory dla synchronizacji kont użytkowników UI i kont posiadaczy kart SKD.
- Integrację urządzenia SIP Intercom (wideodomofon) dla komunikacji dwukierunkowej.
- Możliwość integracji z systemami i bazami danych firm trzecich przez wtyczki (kontrola dostępu, analiza wideo i więcej).
- Dynamiczny podgląd graficzny map.

1.5 Wymagania sprzętowe i oprogramowanie

- Platforma i systemy wbudowane (monitoring CCTV oraz kontrola dostępu KD) powinny być zaprojektowane tak, aby działać na standardowej platformie bazującej na komputerze PC z systemem operacyjnym Windows. Preferowany system operacyjny zostanie uzgodniony z Inwestorem i wybrany spośród systemów operacyjnych obsługiwanych przez producenta.

- Oprogramowanie klient/serwer będzie zbudowane całkowicie używając oprogramowania Microsoft .NET
- Serwer(y) baz danych powinny bazować na programie Microsoft SQL Server. Preferowaną wersję SQL należy uzgodnić z Inwestorem i powinna ona być kompatybilna z istniejącą Platformą w KSP.
- Platforma bezpieczeństwa powinna być kompatybilna ze środowiskami wirtualnymi, w tym VMware oraz Microsoft Hyper-V.

1.6 Architektura

- Projektowana platforma bezpieczeństwa będzie bazowała na modelu klient/serwer i będzie się składała ze standardowego Modułu Oprogramowania Serwera (SSM) i Aplikacji Oprogramowania Klienta (CSA).
- Projektowana platforma bezpieczeństwa powinna być rozwiązaniem pracującym w oparciu o protokół IP. Całość komunikacji pomiędzy SSM a CSA powinna bazować na standardowym protokole TCP/IP i powinna wykorzystywać szyfrowanie TLS z certyfikatami cyfrowymi do zabezpieczenia kanału komunikacji.
- SSM będzie serwisem Windows, który można skonfigurować jako uruchamiany przy włączaniu systemu operacyjnego i będący uruchomionym w tle. SSM będzie uruchamiał się automatycznie przy starcie komputera, niezależnie czy użytkownik zaloguje się do maszyny lub nie.
- Użytkownik będzie mógł uruchomić SSM na pojedynczym serwerze lub na serii kilku serwerów w architekturze rozproszonej.
- Projektowana platforma bezpieczeństwa będzie chroniła przed potencjalną awarią serwera bazy danych i będzie kontynuowała działanie przy użyciu standardowych, ogólnodostępnych rozwiązań.
- Projektowana platforma bezpieczeństwa będzie wspierała min. 10 jednoczesnych połączeń Aplikacji Oprogramowania Klienckiego (CSA) w tym samym momencie.
- Projektowana platforma bezpieczeństwa będzie wspierała nieograniczoną ilość logów i transakcji historycznych (zdarzeń i alarmów) z dozwolonym maksimum będącym limitowanym przez ilość miejsca dostępnego na dysku twardym.
- Projektowana platforma bezpieczeństwa będzie wspierała nieprzerwane przesyłanie strumieniowe wideo. CSA będzie utrzymywało istniejące aktywne połączenia wideo w przypadku niedostępności SSM (za wyjątkiem roli Archiwizowania).

1.7 Aplikacje Oprogramowania Klienta - CSA

- Aplikacje oprogramowania klienta (CSA) będą zapewniały interfejs użytkownika do konfiguracji i monitorowania KD, CCTV i videdomofonu poprzez dowolną sieć, dostępną lokalnie lub ze zdalnego połączenia.
- CSA będą się składały z Konfiguracyjnego UI do konfiguracji systemu i Nadzorczego UI.
- CSA będą bazowały na systemie Windows i będą zapewniały prosty w użyciu, graficzny interfejs użytkownika (UI).

- Administrator Serwera będzie używany do konfiguracji baz(y) danych serwera. Będzie rozwiązaniem sieciowym, dostępnym lokalnie na SSM lub poprzez sieć.
- CSA będą scalać w jednolitą całość funkcjonalności kontroli dostępu KD wraz wideodomofonem i monitoringu CCTV wewnątrz tej samej aplikacji klienckiej.
- Ujednolicona platforma bezpieczeństwa będzie używała najnowszych technologii rozwoju i programowania interfejsu użytkownika (UI) takich jak: WPF (Windows Presentation Foundation), języka znaczników XAML i oprogramowania .NET.
- Wszystkie aplikacje będą zapewniały mechanizm uwierzytelniania, który będzie weryfikował użytkownika. Administrator (mający wszystkie prawa i uprawnienia) może zdefiniować specyficzne prawa dostępu i uprawnienia dla każdego użytkownika systemu.
- Logowanie do CSA będzie wykonywane przez lokalnie składowane konta i hasła użytkowników przy użyciu list uwierzytelniających Windows, jeśli włączona zostanie integracja z Active Directory.

1.8 Konfiguracyjny Interfejsu Użytkownika UI - *ConfigTool*

- Aplikacja Konfiguracyjnego UI będzie pozawalała administratorowi lub użytkownikom z odpowiednimi uprawnieniami zmianę konfiguracji systemu. Konfiguracyjne UI zapewni zdecentralizowaną konfigurację i administrację systemu KD, CCTV i videodomofonu z dowolnego miejsca sieci IP.
- Konfiguracja wszystkich osadzonych systemów KD, CCTV i videodomofonu będzie dostępna przez Konfiguracyjne UI.
- Konfiguracyjne UI będzie posiadało Stronę Domową z dostępem jednym kliknięciem do różnych zadań.
- Konfiguracyjne UI będzie zawierało zbiór narzędzi takich jak narzędzia rozwiązywania problemów, narzędzia importu oraz narzędzie wykrywania jednostek.
- Konfiguracyjne UI będzie zawierać interfejs raportowania statycznego do:
    - Podglądu zdarzeń historycznych bazując na aktywności jednostki. Użytkownik będzie w stanie przeprowadzić działania takie jak drukowanie raportu i rozwiązywanie problemu z konkretnego zdarzenia dostępu z widoku raportowania.
    - Podglądu ścieżki audytów pokazujących historię zmian użytkownika / administratora na jednostce.
    - Wspólne jednostki takie jak użytkownicy, harmonogramy, alarmy i inne, mogą zostać użyte ponownie przez wszystkie osadzone systemy (SKD, CCTV).

1.9 Nadzorczy Interfejs Użytkownika UI – *Security Desk*

- Nadzorczy UI będzie wypełniał rolę Ujednoliconego Interfejsu Zabezpieczeń, zdolnego do monitorowania wideo i dostępu do zdarzeń i alarmów, jak i podglądu na żywo i zapisanego wideo.

- Nadzorczy UI zapewni graficzny interfejs użytkownika do sterowania i monitorowania Platformą przez dowolną sieć IP. Umożliwi administratorom i operatorom z odpowiednimi uprawnieniami monitorowanie ich ujednoliconą platformę zabezpieczeń, wydruk raportów i zarządzanie alarmami.
- Nadzorcze UI będą wspierać następujące koncepcje, aby zwiększyć użyteczność i wydajność operatorów:
  - Dynamicznie adaptujący się interfejs użytkownika, który dostosowuje się w czasie rzeczywistym do działań operatora.
  - Dynamiczny panel sterowania z załadowanymi widżetami zależnymi od jednostek, np. widżet drzwi i kamery.
  - Użycie przezroczystych nakładek, które są w stanie wyświetlić wiele danych w prosty sposób.
  - Wyświetlanie menu kafelkowych i szybkich komend.
  - Menu kafelkowe i szybkie komendy łatwo dostępne wewnątrz każdego kafelka środowiska pracy użytkownika.
  - Funkcjonalność jednego kliknięcia do raportowania i śledzenia. Nadzorcze UI będzie wspierało raportowanie jednym kliknięciem dla kontroli dostępu i wideo, jak również śledzenie jednym kliknięciem obszarów, kamer, drzwi, stref, posiadaczy kart. Raportowanie i śledzenie jednym kliknięciem będzie tworzyło nowe zadanie z wybranymi jednostkami do raportowania lub śledzenia.
- Cykle pracy operatora
  - Cykl pracy będzie sekwencją działań operatora lub administratora których wykonanie doprowadzi do zakończenia działania. „Cykl" odpowiada jasno zdefiniowanemu porządkowi chronologicznemu lub sekwencji wykonującej działanie.
  - Nadzorczy UI będzie wyposażony w spójne cykle pracy dla systemów wideo i kontroli dostępu które ujednolica.
  - Generowanie lub wydruk raportu, ustawianie lub potwierdzanie alarmu, tworzenie raportu zdarzenia powinno przebiegać w ten sam sposób (cykl pracy) bez względu czy operator pracuje z wideo lub kontrolą dostępu, lub wideo razem z kontrolą dostępu.
- Każde zadanie wewnątrz Nadzorczego UI składa się z jednego lub większej ilości następujących elementów:
  - Lista zdarzeń.
  - Drzewo logiczne. Drzwi, kamery, strefy będą pogrupowane pod Obszarami w sposób hierarchiczny.
  - Lista upoważnień wszystkich monitorowanych upoważnień.
  - Wyświetlanie kafelek w różnych wzorach ((1 x 1, 2 x 2, i więcej).
  - Wyświetlanie menu kafelkowych z różnymi komendami powiązanymi z drzwiami, kamerami, PTZ i elementami sterującymi kafelek.
  - Panel sterowania z widżetami.

- Nadzorczy UI będzie wspierał wiele list zdarzeń i wyświetlał wzory kafelek, zawierające:
  - Tylko układ listy zdarzeń/alarmów
  - Tylko wyświetlenie układu kafelków
  - Połączenie wyświetlania układu kafelków z listą zdarzeń/alarmów
- Dostosowywanie obszaru pracy użytkownika
  - Użytkownik będzie posiadał pełną kontrolę nad swoim obszarem pracy przez różne opcje dostosowujące. Administratorzy będą w stanie ograniczyć zdolność modyfikacji użytkowników i operatorów w ich obszarach pracy za pomocą uprawnień.
  - Po dostosowaniu, użytkownik będzie w stanie zapisać stan swojego obszaru.
  - Obszar pracy użytkownika będzie dostępny dla konkretnego użytkownika z dowolnej aplikacji klienckiej w sieci.
  - Wzory wyświetlania kafelek będą dostosowywane.
  - Lista zdarzeń lub alarmów będzie rozwijać się od części ekranu aż do całego ekranu i jej rozmiar będzie mógł zostać zmieniony przez użytkownika. Długość listy zdarzeń lub alarmów będzie definiowana przez użytkownika. Paski przewijania umożliwiają użytkownikowi nawigację przez długie listy alarmów i zdarzeń.
  - Nadzorczy UI wspiera wiele wzorów wyświetlania kafelek, np. 1 kafelek wyświetlający (macierz 1x1), 16 kafelek (macierz 8x8) i wiele dodatkowych kombinacji.
  - Nadzorcze UI wspiera wiele i taką ilość monitorów, jaką jest w stanie zaakceptować adapter wideo komputera i system operacyjny Windows.
  - Dodatkowe opcje dostosowujące zawierają: pokazanie/ukrycie sekcji okna, pokazanie/ukrycie menu/pasków narzędzi, pokazanie/ukrycie informacji na wideo, zmiana rozmiaru różnych sekcji okna, wybór wzory wyświetlania kafelków w trybie zadaniowym.
- Nadzorcze UI zapewnia interfejs do wspomagania następujących działań wspólnych dla kontroli dostępu i wideo:
  - Monitorowanie zdarzeń z systemu zabezpieczeń na żywo (CCTV i/lub KD).
  - Generowanie raportów, włączając w to niestandardowe raporty.
  - Monitorowanie oraz potwierdzanie alarmów.
  - Tworzenie i edycja zdarzeń i generowanie raportów zdarzeń.
  - Wyświetlanie dynamicznych map graficznych i planów pięter.
  - Wykonywanie działań z dynamicznej mapy graficznej i planów pięter.
  - Zarządzanie i wykonywanie na żywo działań i makr.

- Nadzorcze UI będzie zdolne do monitorowania działań następujących jednostek w czasie rzeczywistym przez zadanie nadzorcze, między innymi: obszary, jednostki, drzwi, kamery, posiadacze kart, grupy posiadaczy kart, strefy (punkty wejść), i więcej.
- Nadzorcze UI zapewnia interfejs do wspomagania następujących zadań kontroli dostępu:
  - Monitorowanie i zarządzanie zdarzeniami dostępu i alarmami.
  - Podgląd zdjęć posiadaczy kart lub identyfikatorów przepustek.
  - Weryfikacja zdjęć identyfikatorów posiadaczy kart z nagraniem wideo.
  - Zbieranie i liczenie ludzi, włączając w to resetowanie ilości ludzi przebywających na obszarze
  - Sterowanie drzwiami (zdalne otwieranie drzwi, unieważnianie harmonogramów otwierania drzwi, włączanie trybu konserwacji drzwi).
  - Zwalnianie zabezpieczenia powtórnego użycia karty.
  - Generacja raportów konfiguracji i aktywności KD.
  - Podgląd plików HTML zawierających instrukcje alarmowe.
- Nadzorczy UI będzie zawierał zaawansowane możliwości wideo:
  - Zaawansowaną funkcjonalność podglądu wideo na żywo.
  - Zaawansowaną funkcjonalność odtwarzania nagrań wideo i nagrań zarchiwizowanych.
  - Monitorowanie i zarządzanie zdarzeniami systemu wideo i alarmami.
  - Intercom i audio dwukierunkowe.
  - Generacja raportów wideo.
  - Sterowanie kamerami PTZ.
  - Tworzenie i monitorowanie żądań transferu archiwum;
  - Wyświetlanie metadanych nałożonych na wideo na żywo lub odtwarzane z nagrania;
- Możliwości podglądu na żywo wideo Nadzorczego UI zawierają:
  - Wyświetlanie wszystkich kamer połączonych z systemem.
  - Monitorowanie wideo na żywo na każdym kafelku wyświetlającym wewnątrz zadania w obszarze roboczym użytkownika.
  - Nieprzerwane przesyłanie strumieniowe wideo. CSA będzie utrzymywało istniejące aktywne połączenia wideo w przypadku niedostępności SSM (za wyjątkiem Archiwizowania).
  - Operator będzie w stanie przeciągnąć i upuścić kamerę na kafelek wyświetlający, aby uzyskać podgląd na żywo.
  - Operator będzie w stanie przeciągnąć i upuścić kamerę na kafelek wyświetlający, aby uzyskać podgląd na żywo na analogowym

monitorze połączonym to sprzętowego dekodera IP (konwertującym zakodowany strumień IP na analogowy sygnał wideo).

- Operator będzie w stanie przeciągnąć i upuścić kamerę z mapy na kafelek wyświetlający, aby uzyskać podgląd na żywo.
- Będzie wspierał cyfrowe przybliżanie na strumieniach video na żywo.
- Będzie pozwalał na komunikację audio z jednostkami wideo przez wejście i wyjście audio.
- Operator będzie w stanie sterować przechyłem-odchyleniem-przybliżeniem, przysłoną, ostrością i nastawami.
- Będzie pozwalał operatorom na zapisanie ważnych zdarzeń do późniejszego odzyskania na dowolnej kamerze archiwizującej. Operatorzy mogą nazywać w sposób unikalny każdy zapis, aby ułatwić późniejsze poszukiwania.
- Operator będzie w stanie uruchomić/zatrzymać nagrywanie dowolnej kamery w systemie, która została skonfigurowana z możliwością nagrywania manualnego, przez pojedyncze kliknięcie przyciskiem.
- Operator będzie miał możliwość aktywowania lub dezaktywacji podglądu wszystkich zdarzeń systemu w trakcie ich występowania.
- Będzie pozwalać operatorom na przełączenie na szybką powtórkę nagrania dowolnej kamery archiwizującej za pomocą pojedynczego kliknięcia przycisku.
- Użytkownicy będą w stanie wykonywać zrzuty z wideo na żywo i będą w stanie zapisywać lub drukować zrzuty.
- Użytkownicy będą w stanie podglądać tę samą kamerę wiele razy w różnych kafelkach.

- Możliwości odtwarzania wideo (odtwarzanie zarchiwizowanych nagrań) Nadzorczego UI zawierają:
  - Będzie wspierać odtwarzanie dźwięku i wideo z dowolnego okresu czasu.
  - Będzie pozwalał operatorom na przełączenie na szybką powtórkę nagrania dowolnej kamery archiwizującej za pomocą pojedynczego kliknięcia przycisku.
  - Będzie umożliwiał operatorowi na wybór pomiędzy natychmiastową synchronizacją wszystkich strumieni wideo w trybie odtwarzania, umożliwiając operatorom podgląd zdarzeń z wielu kątów lub z różnych obszarów kamer, lub na odtwarzanie niesynchroniczne.
  - Będzie umożliwiał na jednoczesny podgląd tej samej kamery w wielu kafelkach w różnych odstępach czasu.
  - Będzie umożliwiał operatorowi sterownie odtwarzaniem za pomocą: pauzy, zablokowanie prędkości, odtwarzanie w przód i wstecz klatka po klatce, powolne odtwarzanie w przód i wstecz, odtwarzanie w pętli pomiędzy dwoma znacznikami w czasie

- Będzie wyświetlał jedną oś czasu lub opcjonalnie jedną oś czasu dla każdego wybranego strumienia wideo, w którym operator może nawigować przez sekwencje wideo przez proste kliknięcie na dowolnym punkcie osi czasu.
- Będzie w stanie odpytywać zarchiwizowane wideo używając różnych kryteriów wyszukiwania, między innymi czasu, daty, kamery i obszaru, między innymi.
- Będzie zapewniał narzędzia do przeszukiwania zapisów wideo i powiązanych zapisów audio na podstawie zdefiniowanych przez użytkownika parametrach działań lub ruchu.
- Będzie umożliwiał operatorom na definiowanie obszaru pola wideo, w którym powinien poszukiwać ruchu, jak również definiować ilość ruchu która wyzwoli wyniki wyszukiwania. Nadzorcze UI następnie odzyskuje wszystkie zarchiwizowane strumienie wideo, które zawierają ruch, który spełnia parametry wyszukiwania. Udostępniona zostanie graficzna oś czasu, gdzie czas każdego trafienia wyszukiwania zostanie oznaczony.
- Umożliwi operatorom przeglądanie przez listę wszystkich zakładek stworzonych na systemie i wybór dowolnej zakładki do podglądu.
- Umożliwi użytkownikowi dodawanie zakładek do wcześniej zarchiwizowanych nagrań wideo do łatwiejszego wyszukiwania i odzyskiwania.
- Będzie wspierał cyfrowe przybliżanie na odtwarzanych strumieniach video.
- Będzie zapewniał eksport statycznych obrazów do formatów PNG, JPEG, GIF i BMP ze stemplem daty, czasu i nazwy kamery na zdjęciu (zrzucie).
- Narzędzia do eksportu wideo oraz samodzielny odtwarzacz wideo na różnych nośnikach, takich jak pamięć USB lub płyty CD/DVD-ROM. Odtwarzacz wideo powinien być łatwy w użyciu bez przeszkolenia i powinien obsługiwać przegląd metadanych wideo, takich jak zakładki, a także nawigację w wideo przy pomocy funkcji, takich jak korekcja dystorsji widoku kamery panoramicznej.
- Będzie zapewniał narzędzia do eksportu sekwencji wideo w standardowych formatach wideo, takich jak ASF i MP4.
- Będzie zapewniał zdolność zakodowywania wyeksportowanych plików wideo.
- Będzie pozwalał operatorom na żądanie dynamicznie blokować strumień wideo dla użytkowników niższego poziomu, zapobiegając dostępowi, na określony czas, do podglądu na żywo i nagrań zarchiwizowanych.
- Możliwość przechowywania eksportowanego wideo i eksportowanego obrazu nieruchomego w określonej wcześniej lokalizacji.

1.10 Raportowanie

- System będzie wspierał generowanie raportów (raportowanie bazy danych) dla kontroli dostępu i wideo.
- Każdy raport w systemie będzie zadaniem z przydzielonymi indywidualnie uprawnieniami. Użytkownik będzie posiadał dostęp do konkretnego zadania raportu, jeśli on/ona będzie posiadał odpowiednie uprawnienie.
- Cykle pracy do tworzenia, modyfikacji i uruchamiania raportu będą spójne dla kontroli dostępu i raportów wideo.
- Kontrola dostępu i raporty wideo będą odpowiednio wspierały zdjęcia posiadaczy kart

1.11 Dynamiczne Mapy Graficzne

- System będzie wspierał funkcjonalność mapowania dla kontroli dostępu, nadzoru wideo i aplikacji zewnętrznych.
- Wykonawca uruchomi interfejs mapowy z możliwością sterowania wszystkimi możliwościami systemu.
- Dynamiczny interfejs mapowy zapewni możliwość wyświetlenia wszystkich rodzimych elementów systemu:
  - kamer
  - drzwi,
  - obszarów,
  - videodomofonów,
  - alarmów
- Dynamiczny interfejs mapowy powinny zapewniać operatorowi możliwość zarządzania warstwami elementów wyświetlanych na mapie, włączania ich i wyłączania, a także zmiany kolejności nakładania.
- Będzie możliwe reprezentowanie fizycznej lokacji obszarów, kamer, drzwi, alarmów, stref (monitorowane wejścia), cyfrowych wejść i wyjść.
- Interfejs mapowy powinny wyświetlać rzeczywiste pole widzenia kamery. Powinna być zapewniona możliwość konfiguracji pola widzenia kamery poprzez wpisanie specyfikacji instalacji kamery lub graficznie poprzez przesunięcie granic pola widzenia.
- Możliwe będzie monitorowanie z interfejsu mapowego wszystkich powiadomień o zdarzeniach dla wszystkich elementów. Użytkownicy powinni być w stanie włączać i wyłączać powiadomienia dla poszczególnych elementów.

Podsystem kontroli dostępu i wideodomofon – KD – *Security Center Synergis*

W celu zabezpieczanie pomieszczeń wymagających szczególnej ochrony i kontroli w obiekcie oraz ograniczenia dostępu osobom postronnym przewiduje się instalację systemu kontroli dostępu – KD wraz z wideodomofonem.

Instalacja kontroli dostępu będzie się składać ze sterowników (kontrolerów) grupy przejść, czytników kart magnetycznych, przycisków otwarcia drzwi (przy jednostronnej kontroli przejścia), przycisków awaryjnego otwarcia drzwi (wyjścia), czujników uprawnionego otwarcia drzwi, rygli lub trzymaczy elektromagnetycznych, czujników kontaktronowych stanu drzwi, serwera sytemu wraz z oprogramowaniem i komputerowych stacji roboczych z zainstalowanym oprogramowaniem klienckim i zarządzającym. Zakłada się, że drzwi objęte kontrolą dostępu będą wyposażone w samozamykacze. Każdy kontroler będzie miał możliwość samodzielnej pracy jak również będzie połączony w sieci ze wszystkimi kontrolerami i centralą (serwerem) zintegrowanego systemu zabezpieczeń (dedykowany komputer z odpowiednim oprogramowaniem dla KD i VMS) zlokalizowany w serwerowni SSK KSP. Oprogramowanie będzie umożliwiało m.in. dowolną rekonfigurację systemu tzn. zmiany nadawania uprawnień dla poszczególnych kart dostępu, rejestrowanie drukowanie raportów.

Oprogramowanie klienckie będzie zainstalowane na dedykowanej stacji roboczej zainstalowanej w docelowym pomieszczeniu służby dyżurnej przeznaczonej dla operatora ujednoliconej platformy bezpieczeństwa.

Centralę (serwer) systemu zamontować w pomieszczeniu serwerowni. Urządzenia kontroli dostępu będą zasilone z tablicy zasilania gwarantowanego. Okablowanie systemu wykonać zgodnie z zalecanymi producentów zastosowanych urządzeń.

Instalacja wideodomofonowa zapewni komunikację pomiędzy drzwiami/furtami/bramami wejściowymi do strefy chronionej i umożliwi dyżurnemu zdalne otwarcie wszystkich drzwi z ww. dedykowanej stacji roboczej.

2.1 Wymagane funkcjonalności dla systemu kontroli dostępu - KD

- KD będzie rozwiązaniem oprogramowania kontroli dostępu klasy IP dla przedsiębiorstw. Będzie w pełni wbudowany w Ujednoliconą Platformę Bezpieczeństwa i umożliwi bezproblemowe ujednolicenie KD z systemem zarządzania video IP (VMS).
- KD będzie skalowalny, aby wspierać konfiguracje składające się z tysięcy drzwi, z obiektami znajdującymi się w wielu obszarach geograficznych.
- Aplikacja do zarządzania i obsługi systemu powinna umożliwiać pracę w trybie 64-bitowym.
- System będzie wspierał nieograniczoną ilość logów i transakcji historycznych (zdarzeń i alarmów) z dozwolonym maksimum będącym limitowanym przez ilość miejsca dostępnego na dysku twardym.
- KD będzie wspierał wiele funkcjonalności kontroli dostępu, między innymi:
  - Zarządzanie sterownikami (jednostkami), zarządzanie drzwiami, zarządzanie i zarządzanie obszarami
  - Zarządzanie posiadaczami kart i grupami posiadaczy kart, zarządzanie listami uwierzytelniającymi i zarządzanie zasadami dostępu
  - Drukowanie identyfikatorów i tworzenie szablonów.

- Zarządzanie odwiedzinami.
- Zliczanie ludzi, śledzenie obecności na obszarze i zbieranie.

- KD będzie wspierał globalne zarządzanie posiadaczami kart i synchronizację pomiędzy centralną niezależną jednostką i zdalną niezależną jednostką, gdzie każda z nich może posiadać własny Katalog i bazy danych.
- Będzie istniała możliwość synchronizacji następujących jednostek i ich baz danych konfiguracji:
  - Posiadacze kart (zawierając pola niestandardowe)
  - Grupy posiadaczy kart
  - Listy uwierzytelniające
  - Szablony identyfikatorów.
- Posiadacze kart i inne synchronizowane jednostki mogą być dodawane centralnie i synchronizowane do zdalnych obiektów dla centralnego zarządzania posiadaczami kart.
- Posiadacze kart i inne synchronizowane jednostki mogą być dodawane w zdalnych obiektach i synchronizowane do obiektu centralnego i innych zdalnych obiektów.
- Będzie wspierał pojedynczą kartę dla jednego posiadacza kart we wszystkich obiektach organizacji.
- Wspierana będzie synchronizacja manualna i z harmonogramem.

2.2 Zarządzanie Posiadaczami Kart i Grupami Posiadaczy Kart

- KD będzie wspierał konfigurację i zarządzanie posiadaczami kart i grupami posiadaczy kart. Użytkownik będzie zdolny do dodawania, usuwania lub modyfikacji posiadacza karty lub grupę posiadaczy kart w przypadku posiadania odpowiednich uprawnień.
- KD będzie pozwalał na następujące opcje aktywacji/wygasania dla profilu posiadacza karty: opóźniona aktywacja profilu posiadacza karty, wygaśnięcie bazując na dacie pierwszego użycia listy uwierzytelniającej lub wygaśnięcie w określonej przez użytkownika dacie
- Możliwe będzie przypisanie zdjęcia do profilu posiadacza karty. Zdjęcie będzie zaimportowane z pliku, uchwycone za pomocą aparatu cyfrowego lub uchwycone za pomocą kamery podsystemu CCTV.
- Kiedy wystąpi zdarzenie posiadacza karty, zdjęcia posiadacza karty zostanie wyświetlone w Nadzorczym UI. KD będzie wspierał wiele standardów formatów zdjęć.
- Grupy posiadaczy kart będą pozwalały na grupowanie posiadaczy kart, aby umożliwić masowe zmiany do ustawień systemu. Możliwe będzie przypisanie grupy posiadaczy kart to zasad dostępu, dzięki czemu nie będzie potrzeby przypisywania każdego posiadacza z osobna.
- Możliwe będzie przeszukiwanie przez przypisanie zdjęcia, niestandardowe pola i nazwiska

- Będzie możliwy wybór wielu posiadaczy kart dla natychmiastowej dezaktywacji lub reaktywacji
- KD będzie wspierał synchronizację posiadaczy kart lub grup posiadaczy kart przez Active Directory, zawierając w tym listy uwierzytelniające i zdjęcie posiadacza karty.
- W ramach inwestycji Wykonawca dostarczy min 2x ilość etatów, magnetycznych kart dla użytkowników projektowanego systemu KD.

2.3 Zarządzanie Drzwiami

- KD będzie wspierał konfigurację i zarządzanie drzwiami. Użytkownik będzie zdolny do dodawania, usuwania lub modyfikacji drzwi w przypadku posiadania odpowiednich uprawnień.
- KD będzie pozawalał na przypisanie wielu zasad dostępu do drzwi.
- KD będzie wspierał następujące formy uwierzytelniania: Tylko Karta, Karta lub Klawiatura (PIN), lub Karta i Klawiatura (PIN). Będzie możliwe definiowanie harmonogramu, kiedy tryby uwierzytelniania Tylko Karta lub Karta i Klawiatura będą wymagane.
- Wydłużony czas dostępu. Będzie możliwe ustawienie przedłużonego czasu dostępu dla każdych drzwi osobno (dodatkowo do ustawienia standardowego czasu dostępu). Właściwości posiadacza karty będą uwzględniać opcję użycia wydłużonego czasu dostępu. Po uzyskaniu dostępu przez oznaczonych posiadaczy kart drzwi pozostaną otwarte przez wydłużony czas dostępu, zamiast standardowego czasu dostępu.
- KD powinien umożliwiać konfigurację trybu ponownego zamykania drzwi zamkiem, takiego jak po otwarciu drzwi, po określonym czasie lub po zamknięciu drzwi.
- KD powinien umożliwiać wymuszanie użycia dwóch ważnych odczytów wykonanych przez różnych posiadaczy kart przed umożliwieniem dostępu do danego obszaru.
- KD powinien umożliwiać aktywowanie reguł dostępu dla innych posiadaczy kart po uzyskaniu do danego obszaru dostępu przez kierownika.
- KD powinien umożliwiać aktywację harmonogramu otwierania zamków w drzwiach po wejściu pracownika do obiektu.
- Harmonogramy otwierania i wyjątki od harmonogramów otwierania będą przypisane do drzwi. Harmonogram otwierania będzie określał, kiedy drzwi powinny być automatycznie otwarte. KD będzie również wspierał użycie konkretnych harmonogramów otwierania bez dostępu do sieci. Wyjątki od harmonogramów otwierania będą używane do definiowania okresów czasu podczas których harmonogramy otwierania nie będą stosowane, np. podczas świąt państwowych.
- KD będzie wspierać jedną lub więcej kamer na drzwi. Wideo będzie wtedy przypisane do zdarzenia dostępu do drzwi, np. uzyskanie dostępu lub odmowa dostępu.

Podsystem monitoringu wizyjnego VMS – CCTV- *Security Center Omnicast*

Jako uzupełnienie systemów KD i videodomofonowego zainstalowany i uruchomiony zostanie system telewizji przemysłowej CCTV. Monitorowaniu podlegać powinny rejony wokół stref chronionych, do których mogą dostać się osoby z zewnątrz, ciągi komunikacyjne, punkt obsługi interesanta, tzw. pomieszczenia przejściowe, parking wewnętrzny, teren przyległy do obiektu; obrazy powinny być rejestrowane do celów dowodowych i przechowywane przez czas wymagany przez Użytkownika.

W wyniku analizy zagrożeń oraz uwzględnienia jakościowego charakteru tychże zagrożeń, do stref wymagających szczególnej ochrony zalicza się:

- wejścia do obiektu,
- ciągi komunikacyjne w obiekcie,
- punkt obsługi interesanta,
- pomieszczenia, gdzie prowadzone są czynności służbowe wobec osób doprowadzonych i ciągi komunikacyjne do tych pomieszczeń,
- wejście do pomieszczenia służby dyżurnej,

Instalacja systemu CCTV będzie się składać z cyfrowych megapikselowych kamer przemysłowych w obudowie wandaloodpornej i/lub typu bullet, przełączników LAN PoE, Każda kamera będzie połączona w sieci z serwerem VMS zintegrowanego systemu zabezpieczeń (dedykowany komputer z odpowiednim oprogramowaniem dla VMS i KD) zlokalizowanym w serwerowni SSK KSP. Oprogramowanie będzie umożliwiało m.in. dowolną rekonfigurację systemu tzn. zmiany ustawień dla poszczególnych urządzeń systemu, rejestrowanie drukowanie raportów. Oprogramowanie klienckie z podglądem obrazu z kamer będzie zainstalowane na dedykowanej stacji roboczej zainstalowanej w docelowym pomieszczeniu służby dyżurnej przeznaczonej dla operatora ujednoliconej platformy bezpieczeństwa.

Centralę (serwer) z zainstalowanym systemem VMS zamontować w pomieszczeniu serwerowni. Okablowanie systemu wykonać zgodnie z zalecanymi producentów zastosowanych urządzeń.

2.4 Funkcjonalności podsystemu monitoringu wizyjnego VMS – CCTV

- VMS będzie bazował na otwartej architekturze, która pozwoli na użycie nie własnościowych urządzeń stacji roboczych i serwerów, nie własnościowej infrastruktury sieciowej oraz nie własnościowych nośników danych.
- VMS oferować będzie pełne i skalowalne rozwiązanie, które pozwali na dodawanie kamer na zasadzie jednostka po jednostce.
- Wszystkie strumienie wideo dostarczane z kamer IP zostaną zakodowany cyfrowo w formatach kompresyjnych MPEG-4, MPEG-2, MJPEG, H.264, H.265, Wavelet lub JPEG2000 i nagrywane jednocześnie w czasie rzeczywistym.
- Wszystkie strumienie audio dostarczane z serwerów video IP (np. wideodomofon, kamera z mikrofonem) zostaną zakodowane cyfrowo w formatach

kompresyjnych g711 (u-law), g721, g723 lub AAC i nagrywane jednocześnie w czasie rzeczywistym.

- VMS będzie wspierał standardy ONVIF do komunikacji z urządzeniami bazujących na protokole sieciowym TCP/IP.
- VMS obsługiwać będzie protokoły kamer PTZ od wielu producentów, w tym protokoły analogowe i IP.
- VMS rozstrzygać będzie konflikty pomiędzy użytkownikami dotyczące użycia kamer PTZ na podstawie poziomu użytkownika dla każdej kamery.
- Konfiguracyjne UI będzie pozawalało administratorowi lub użytkownikom z odpowiednimi uprawnieniami na zmianę konfiguracji ustawień wideo.
- Konfiguracyjne UI będzie zapewniało możliwość zmiany parametrów jakości wideo, przepustowości łącza i częstotliwości wyświetlania klatek na każdej kamerze (strumieniu) z osobna dla podglądu na żywo i nagrywanego wideo.
- Konfiguracyjne UI powinien zapewniać możliwość zmiany jakości wideo poprzez wybór określonego wcześniej wzorca jakości wideo.
- Konfiguracyjne UI będzie zapewniało zdolność ustawienia harmonogramów nagrywania i trybów dla każdej kamery. Dostępne tryby nagrywania:
  - Ciągły
  - W ruchu i manualny
  - Tylko manualny
  - Wyłączony
- Archiwizator (rola w systemie) umożliwiać będzie wielokrotne kodowanie każdej kamery (źródła materiału wideo) w tym samym lub innych formatach wideo (MPEG-4, MPEG-2, MJPEG, H.264, H.265, Wavelet lub JPEG2000), ograniczonych możliwościami każdego urządzenia.
- Archiwizowanie pozwoli na zmianę jakości wideo zgodnie z uprzednio zdefiniowanymi harmonogramami. Harmonogramy będą posiadały tę samą elastyczność konfiguracji co harmonogramy nagrywania wymienione powyżej. Jakość wideo będzie bazowała, ale nie jedynie, na następujących parametrach:
  - Maksymalna szybkość transmisji danych
  - Maksymalna częstotliwość wyświetlanych klatek
  - Jakość obrazu
  - Przedział klatek kluczowych
- Archiwizator udostępnia następujące opcje czyszczenia starych archiwów, na zasadzie kamera po kamerze:
  - Po określonej ilości dni
  - Usuwanie wpierw najstarszych archiwów, kiedy skończy się miejsce na dysku
  - Zatrzymanie archiwizacji, kiedy dyski zapełnią się.
- Archiwizator umożliwi rejestrację obrazu w trybie ciągłym ze wszystkich kamer w systemie VMS i jednocześnie zapewni okres przechowywania nagrań przez okres

min 30 dni, przy założeniu: obraz o rozdzielczości FullHD 2Mpx i 25 kl./s.

2.5 Minimalne parametry techniczne dla kamer w systemie CCTV

Kamer Typ A - Kamera w obudowie kopułowej, wandaloodpornej, 2Mpx, IP66 o parametrach nie gorszych niż:

Przetwornik obrazu:	CMOS
Rozmiar przetwornika:	1/2.8
Rozmiar przetwornika w megapikselach:	2
Min. oświetlenie (obraz kolorowy):	0.1 lux
Min. oświetlenie (obraz czarno-biały):	0 lux
WDR:	tak
Parametry wideo	
Rozdzielczość obrazu wideo:	1920xx1080
Liczba klatek na sekundę:	50
Tryb pracy dzień/noc:	tak
Parametry obiektywu	
Długość ogniskowej:	3.4 – 8.9 mm
Pole widzenia w poziomie:	100-36°
Pole widzenia w pionie:	53-20°
Parametry kompresji obrazu	
Ilość strumieni wideo:	2
Kodowanie wideo:	H.264, H.265, MJPEG
Parametry audio	
Obsługa audio:	tak, złącze do podłączenia zewnętrznego mikrofonu
Kodowanie audio:	24bit LPCM, AAC-LC 16/32/44.1/48kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz
Parametry IP	
Wspierane Protokoły:	IPv4, IPv6 USGv6, HTTP, HTTPSa, TTP/2, SSL/TLSa, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, SIP, LLDP, MQTT, Syslog
Ogólne	
Zdalne ustawienie ostrości:	tak
Zdalny zoom:	tak

Wbudowany oświetlacz podczerwieni:	tak, 40 m
Zakres temp. pracy:	od -40 do 50 °C
Klasa odporności na wandalizm:	IK10
Klasa szczelności:	IP66
Zasilanie:	Power over Ethernet 802.3at, 12V DC

Kamera Typ B - Kamera w obudowie bullet, 2Mpx o parametrach nie gorszych niż:

Przetwornik obrazu:	CMOS
Rozmiar przetwornika:	1/2.8
Rozmiar przetwornika w megapikselach:	2
Min. oświetlenie (obraz kolorowy):	0.07 lux
Min. oświetlenie (obraz czarno-biały):	0.01 lux
WDR:	tak
Parametry wideo	
Rozdzielczość obrazu wideo:	1920xx1080
Liczba klatek na sekundę:	50
Tryb pracy dzień/noc:	tak
Parametry obiektywu	
Długość ogniskowej:	3 – 9 mm
Pole widzenia w poziomie:	114-37°
Pole widzenia w pionie:	58-21°
Parametry kompresji obrazu	
Ilość strumieni wideo:	8
Kodowanie wideo:	H.264, H.265, MJPEG
Parametry audio	
Obsługa audio:	tak, złącze do podłączenia zewnętrznego mikrofonu
Kodowanie audio:	24bit LPCM, AAC-LC 8/16/32/44.1/48kHz, G.711 PCM 8 kHz, G.726 ADPCM 8 kHz
Parametry IP	
Wspierane Protokoły:	IPv4, IPv6 USGv6, HTTP, HTTPSa, HTTP/2, SSL/TLSa, QoS Layer 3 DiffServ, FTP, SFTP, CIFS/SMB, SMTP, Bonjour, UPnP®, SNMPv1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, RTSP, RTP, SRTP, TCP, UDP, IGMP, RTCP, ICMP, DHCPv4/v6, ARP, SOCKS, SSH, SIP, LLDP,MQTT, Syslog

Ogólne

Zdalne ustawienie ostrości:	tak
Zdalny zoom:	tak
Wbudowany oświetlacz podczerwieni:	tak, 40 m
Zakres temp. pracy:	od -40 do 60 °C
Klasa odporności na wandalizm:	IK10
Klasa szczelności:	IP66
Zasilanie:	Power over Ethernet 802.3at, 12V DC

3.3 Minimalne parametry dla rejestratora obrazu z platformą VMS i licencjami kamer.

Podstawowe wymagania oprogramowania platformy VMS:

- Wyświetlanie strumieni wideo na żywo
- Rejestracja strumieni wideo
- Monitorowanie na żywo strumieni z kamer oraz dostęp do zarejestrowanego materiału wideo
- Monitorowanie zdarzeń na żywo
- Zarządzanie alarmami
- Raportowanie, włącznie z tworzeniem własnych szablonów raportów oraz raportowaniem incydentów
- Utworzenie federacji dla globalnego monitorowania, raportowania oraz zarządzania alarmami wielu zdalnych, niezależnych systemów VMS rozlokowanych w wielu obiektach w różnych rejonach Polski.
- Integrację z Microsoft Active Directory dla synchronizacji kont użytkowników
- Integracja z zewnętrznymi systemami i bazami danych przez wtyczki (plug-ins)
- Wyświetlanie dynamicznych map do wizualizacji lokalizacji i stanów urządzeń
- Zarządzania wieloma lokalizacjami / wieloma klientami
- Nadzór / konfiguracja poprzez smartfony i tablety
- Nadzór / konfiguracja poprzez klientów www
- Wbudowana zaawansowana detekcja ruchu
- Obsługa zaawansowanej analityki wideo (po stronie kamer)
- Obsługa analityki wideo pochodzącej od zewnętrznych dostawców (co najmniej 5 różnych dostawców)
- Monitorowanie stanu systemu
- Redundancja oraz backup bazy danych
- Automatyczne przełączanie awaryjne pomiędzy serwerami rejestracji
- Automatyczne przełączanie awaryjne pomiędzy serwerami zarządzania
- Zarządzanie kontami użytkowników i administratorów
- Zarządzanie prawami dostępu do systemu dla użytkowników lokalnych i zdalnych
- Zarządzanie prawami dostępu do materiałów wideo dla użytkowników lokalnych i zdalnych
- Zarządzanie priorytetami dostępu i sterowania w oparciu o priorytety kont użytkowników
- Integracja z różnymi kamerami IP oraz klawiaturami IP

Licencjonowanie

- Platforma posiadającą niezbędne licencje do podłączenia kamer. Platforma posiadająca min. 5 licencji na dołączenie stacji klienckich. Wszystkie licencje wbudowane na centralnym serwerze (rejestratorze) odpowiedzialnym za konfigurację.
- Nie ma konieczności stosowania licencji na stacji klienckiej (licencjonowana jest liczba jednocześnie aktywnych klientów)

Architektura platformy VMS

Oprogramowanie platformy VMS musi być oprogramowaniem pracującym w architekturze klient-serwer. Część serwerowa musi odpowiadać za wszystkie procesy związane z rejestracją i zarządzaniem oraz udostępnianiem danych do stacji klienckich, natomiast część kliencka ma odpowiadać jedynie za pobieranie i wizualizowanie tych danych. Serwer platformy może zostać uruchomiony na pojedynczym serwerze lub na kilku serwerach w rozproszonej architekturze.

- Platforma VMS bazuje na rozwiązaniach IP. Cała komunikacja między serwerem a aplikacją kliencką oparta jest na standardowym protokole TCP/IP wraz z możliwością uruchomienia szyfrowania
- Server platformy VMS pracuje jako usługa Windows w taki sposób, aby uruchamiała się wraz ze startem systemu operacyjnego i pracowała w tle,
- Rozwiązanie ma wspierać koncepcję federacji, w której wiele niezależnych instalacji VMS może być połączonych w jeden duży wirtualny system scentralizowanego monitorowania, raportowania i zarządzania alarmami.

Architektura platformy VMS powinna umożliwiać pełną skalowalność i umożliwiać rozbudowę systemu do:

- Co najmniej 100 serwerów rejestracji i zarządzania
- Co najmniej 100 stacji klienckich
- Co najmniej 500 kamer
- Co najmniej 500 modułów wejść/wyjść alarmowych

Aplikacja kliencka

- Aplikacja kliencka zapewnia interfejs użytkownika dla konfiguracji i monitorowania w dowolnej sieci, dostępnej lokalnie lub poprzez połączenie zdalne.
- Wszystkie aplikacje posiadają mechanizm autoryzacyjny, który weryfikuje użytkownika. Dzięki temu administrator (posiadający wszelkie prawa i przywileje) może zdefiniować określone prawa dostępu dla każdego użytkownika w systemie.
- Logowanie do aplikacji klienta przebiega poprzez konta i hasła platformy przechowywane lokalnie lub poprzez uwierzytelnienia użytkownika Windows, gdy integracja z Active Directory jest włączona.
- Aplikacja musi mieć możliwość wymuszenia na użytkowniku logowanie się razem z jego przełożonym lub administratorem, posiadającym wyższe prawa w hierarchii systemu. Logowanie w takim przypadku polega na wprowadzeniu w tym samym oknie aplikacji danych do logowania zarówno użytkownika jak i administratora. W przypadku niewprowadzania danych do logowania przez administratora, użytkownik nie będzie w stanie się zalogować.
- Aplikacja kliencka dostępna jest co najmniej w językach: angielski i polski,

- W celu usprawnienia użytkowania i efektywności w aplikacji klienckiej zaimplementowano dla czynności administrator/użytkownik podejście zorientowane zadaniowo. Operator może uruchamiać określone zadanie tylko, jeśli posiada do tego określone uprawnienia. Poprzez wykorzystanie uprawnień możliwe jest ukrywanie zadań, do których operator nie może mieć dostępu.

Oprogramowanie stacji klienckiej umożliwi zastosowanie modułu konfiguratora do zarządzania, konfiguracji oprogramowania, do nadzoru oraz do automatycznego i ręcznego raportowania stanu systemu oraz stanu urządzeń peryferyjnych.

Opcje odtwarzania wideo z aplikacji klienckiej z panelu monitoringu (przegląd archiwum) obejmują:

- Odtwarzanie audio i wideo z dowolnego zakresu czasu.
- Odtwarzanie wideo na dowolnym ekranie.
- Wybór pomiędzy odtwarzaniem niezsynchronizowanym lub natychmiastową synchronizacją wszystkich strumieni wideo w trybie odtwarzania, co pozwala na przeglądanie zdarzeń z wielu pozycji lub jako niezsynchronizowany.
- Jednoczesne odtwarzanie tej samej kamery na wielu ekranach w różnych przedziałach czasowych.
- Kontrolowanie odtwarzania dzięki:
  - Pauzie
  - Zablokowanej prędkości
  - Przewijaniu w przód i tył z prędkością: 1x, 2x, 4x, 6x, 10x, 40x, 100x.
  - Przewijaniu w przód i tył klatka po klatce
  - Powolnym przewijaniu w przód i tył z prędkością: 1/8x, 1/4x, 1/2x.
  - Zapętleniu odtwarzania pomiędzy dwoma znacznikami
- Wyświetlanie pojedynczego paska czasu lub jednego paska czasu dla każdej wybranej sekwencji wideo, dzięki któremu możliwa jest nawigacja wzdłuż sekwencji wideo poprzez kliknięcie w dowolnym punkcie paska czasu.
- Wyświetlanie wielkości (poziomu) ruchu w dowolnym przedziale czasu.
- Wyraziście wskazanie zakładek zdarzeń na osi czasu.
- Wyszukuje zarchiwizowane wideo za pomocą zapytań i różnych kryteriów wyszukiwania, w tym czasu, daty, kamery, obszaru i innych.
- Udostępnia narzędzie wyszukiwania zdarzeń zdefiniowanych przez użytkownika lub według parametrów detekcji ruchu pośród plików wideo i powiązanych plików dźwiękowych.
- Wyszukiwanie w liście zakładek utworzonych w systemie i wybranie dowolnego zdarzenia do przeglądania.
- Dodawanie zakładek do wcześniej nagranego wideo w celu łatwiejszego wyszukiwania i selekcji.
- Zoom cyfrowy w przeglądanej sekwencji wideo.
- Eksportowanie zdjęć w formacie PNG, JPEG, GIF i BMP z oznaczeniem daty i czasu, a także nazwą kamery na obrazie (stop klatek).
- Eksportowanie sekwencji video i audio w standardowych formatach wideo np. ASF oraz formatu natywnego producenta platformy ze znacznikami daty i czasu w obrazie. Możliwe jest szyfrowanie eksportowanych sekwencji video. Możliwe jest dodawanie zabezpieczenia w postaci tzw. znaku wodnego do eksportowanego materiału.
- Narzędzia do eksportu wideo na różnych nośnikach, takich jak CD-ROM.

Integracja kamer i urządzeń do oprogramowania platformy VMS

- VMS oparty jest na strukturze otwartej, która umożliwia wykorzystanie będących w powszechnej dystrybucji stacji klienckich, serwerów urządzeń infrastruktury sieci oraz pamięci masowych.
- VMS zapewni pełne i skalowalne oprogramowania nadzoru wideo, które umożliwia dodawanie kamer.
- VMS obsługujący enkodery wideo (wideoserwery) przetwarzające analogowe sygnały wideo na strumienie cyfrowe oraz kamery IP, nazywanymi cyfrowymi źródłami video. VMS współpracuje z enkoderami i kamerami IP wielu producentów.
- Wszystkie strumienie wideo z kamer analogowych lub kamer IP są kodowane cyfrowo w jednym ze standardów kompresji MPEG-4, MPEG-2, MJPEG, H.264, H.265.
- Wszystkie pliki audio z serwerów wideo IP są kodowane cyfrowo jako g711 (u-law), g721, g723 lub AAC i jednocześnie nagrywane w czasie rzeczywistym.

Rejestrowanie

- Zasoby sprzętowe rejestratora (przestrzeń dyskowa HDD) muszą pozwalać na rejestrację strumienia wideo z wszystkich kamer IP o parametrach: rozdzielczość 1920x1080, 25 klatek/sek., bitrate 4500kbps przez okres min. 30 dni kalendarzowych.
- Rola Rejestratora wideo wykorzystuje bazę danych zdarzeń i stempli czasowych w celu zaawansowanego wyszukiwania audio/wideo. Rola rejestratora zbudowana w oparciu o bazę danych to Microsoft SQL Server 2012/2014/2016/2017/2019 Express/Standard/Enterprise
- Rejestrator zabezpiecza zarchiwizowane pliki audio/wideo i bazę danych systemu przed dostępem sieciowym użytkownika bez praw administratora.
- Rejestrator cyfrowo podpisuje zapisane wideo za pomocą kryptograficznego, 124-bitowego klucza RSA typu publiczny/prywatny.
- Rejestrator wykrywa enkodery i kamery IP w innych segmentach sieci, łącznie z Internetem oraz w sieciach używających (lub nie) translacji adresu sieciowego (NAT).
- Rejestrator może konfigurować odstęp klatek kluczowych (I-frame) w sekundach lub w liczbie klatek.
- Rejestrator posiada opcję nagrywania przed lub po alarmie, która może być ustawiona od 1 sekundy do 3 minut dla każdej kamery oddzielnie.
- Rejestrator posiada opcję przechowywania plików wideo i audio na podstawie zdarzeń takich jak:
  - wykrycie ruchu
  - makra
- Rejestrator wykrywa ruch wideo dla każdej kamery osobno, zgodnie z siatką wykrywania ruchu składającą z ponad 1200 bloków wykrywających ruch. Wszystkie ustawienia wykrywania ruchu wideo są konfigurowalne zgodnie ze harmonogramem. Ogólny próg wykrywalności umożliwia zmniejszenie czułości wykrywania ruchu tam, gdzie sygnał wideo jest zakłócony lub tam, gdzie występuje wiele błędnych trafień.
- Rejestrator umożliwia kodowanie każdej kamery (źródła wideo) wielokrotnie w tym samym lub różnych formatach wideo MPEG-4, MPEG-2, MJPEG, H.264, H.265 co ograniczone jest jedynie przez możliwości każdego ze źródeł strumienia IP (enkoder, kamera IP). Gdy dostępne jest wiele strumieni wideo z

tej samej kamery, użytkownicy mogą wybrać dowolny z nich zgodnie z przypisaną im funkcją.

- Rejestrator umożliwia administratorowi określenie ilości miejsca na dysku, które jest zajęte przez chronione wideo.
- Rejestrator może zmniejszać wielkość obrazów wideo w celu oszczędzania miejsca na dysku. Możliwe jest zmniejszenie wielkości strumienia poprzez zmniejszanie ilości klatek kluczowych w kompresjach H.264, MPEG-4, MJPEG.

Przesyłanie strumieni Wideo

- W platformie VMS występuje oddzielna rola/mechanizm odpowiedzialna za routowanie wideo i audio w sieci lokalnej i rozległej ze źródła cyfrowego (enkoder, kamera IP) do celu (np. aplikacji klienckiej).
- Mechanizm ten współpracuje z wieloma protokołami transmisji, takimi jak unicast TCP, unicast UDP oraz multicast UDP. Współpracuje z IGMP (Internet Group Management Protocol) aby ustalić przynależność grup multicastowych.
- Możliwa jest konwersja przekaz z dowolnego obsługiwanego protokołu przekazu, tj.:
  - Multicast UDP do Unicast TCP
  - Multicast UDP do Unicast UDP
  - Unicast TCP do Multicast UDP
  - Unicast UDP do Multicast UDP
- Funkcjonalność przesyłania obrazu ze źródła do celu IP może być chroniona przed niedostępnością sprzętu lub oprogramowania poprzez konfigurację stand-by.
- Kiedy używamy strumienia Multicast z kamery, VMS musi zezwolić na przesłanie strumienia "na żywo" bezpośrednio z kamery do aplikacji klienckiej, omijając przy tym transfer do rejestratora.

Zakres integracji Sytemu Sygnalizacji i Włamania SSWiN

- Integracja SSWiN umożliwi bezpośrednie połączenie między centralą alarmową SSWiN a zunifikowaną platformą bezpieczeństwa (VMS, SKD).
- Integracja będzie realizowana za pośrednictwem sieci IP, z wykorzystaniem szyfrowania.
- Po uruchomieniu, operator zunifikowanej platformy bezpieczeństwa (VMS, SKD) może obsługiwać strefy SSWiN centrali (uzbrajać/rozbrajać), pomijać/odblokowywać wejścia i monitorować alarmy, strefy i stany wejść.
- Monitorowanie stref i wejść będzie zintegrowane z systemem zarządzania materiałem wizyjnym VMS platformy bezpieczeństwa, dzięki czemu alarmy, zdarzenia panelu i raporty mogą być przeglądane wraz z obrazem z kamery w celu weryfikacji.
- Obszary włamań i dane wejściowe będą dynamicznie aktualizowane na mapach Menedżera planów (Plan Manager) przy użyciu niestandardowych ikon i efektów halo.
- Możliwa będzie synchronizacja/zarządzanie (dodawanie/usuwanie) użytkowników centrali bezpośrednio z poziomu interfejsu zunifikowanej platformy bezpieczeństwa (VMS, SKD) i przypisywanie haseł do central alarmowych.

- Obszary włamań będą monitorowane i obsługiwane z systemu federacyjnego – istniejącego nadrzędnego (centralnego) systemu VMS uruchomionego w Komendzie Stołecznej Policji.
- Integracja z centralą SSWiN pozwali na wykorzystanie wszystkich funkcji zunifikowanych systemów platformy bezpieczeństwa (mechanizm od zdarzeń do działań – event to action, panel podsumowania SSWiN i inne widżety, raportowanie incydentów poprzez moduł Clearance, SKD itp.)

System Wideodomofonowy

System Wideodomofonowy KSP stosuje się we wszystkich typach obiektów KSP, KRP, KPP,KP i PP. W przypadku obiektów czynnych czasowo (np. 8.00 – 16.00) po godzinach pracy jednostki Policji wywołanie z Wideodomofonu zostaje przekierowane do jednostki nadrzędnej KPP lub KRP do Służby Dyżurnej obiektu nadrzędnego.

Montowany system wideo-domofonowy musi spełniać następujące wymagania:

1. Posiadać możliwość rozbudowy na obiekty podległe działające w rozległych sieciach (WAN) Zamawiającego,
2. Transmisja nie może zajmować pasma większego niż 2 Mbit/s,
3. Zapewniać kompatybilność ze stosowanymi urządzeniami, ze szczególnym uwzględnieniem CISCO CUCM v. 8.6.2.oraz 9.1.2 oraz przygotowany współpracy z v. 12.5,
4. Musi zapewniać połączenie bezpośrednie SIP,
5. Musi wspierać protokoły: SIP 2.0 (RFC 3261) /TCP/IP/UDP, RTP/HTTP/ARP, ICMP DHCP DNS, TFTP, NTP,
6. Musi posiadać kodowanie głosu G.711 (A/u-law),
7. Musi posiadać kodowanie obrazu H.264 wideokodek czasu rzeczywistego w rozdzielczościach: QCIF, QVGA, CIF, VGA; obsługiwane 30 klatek na sekundę,
8. Musi posiadać możliwość zasilania PoE (IEEE 802.3.af),
9. Musi być wyposażony być w zasilacz PoE,
10. Musi posiadać możliwość dostępu do programowania i konfiguracji przez przeglądarkę WWW.

Panele zewnętrzne muszą posiadać:

1. Klasę szczelności nie mniejszą niż IP 53,
2. Odporność na warunku atmosferyczne. Temperatura pracy nie gorsza niż w granicach od -20^{0}C do +60^{0}C.

System Sygnalizacji Włamania i Napadu SSWiN

1. SSWiN powinien być przygotowany wg obowiązujących przepisów. Przy projektowaniu należy uwzględnić PN-EN 50131-1:2009 jak również normy i przepisy dotyczące konkretnych pomieszczeń.
2. Projektowany system alarmowy musi być w pełni kompatybilny (tj. umożliwiać zarządzanie uprawnieniami użytkowników systemu, strefami; umożliwiać wyświetlanie

stanu stref, wejść, wyjść oraz zdarzeń w systemie, jak również umożliwiać zdalne zazbrajanie / rozbrajanie systemu) z obecnie wykorzystywanymi platformami / aplikacjami zarządzania systemami bezpieczeństwa tj. Integrum, Dloadx, GuardX, jak również stacją monitorującą Stam.

3. SSWiN powinien być przygotowany wg obowiązujących przepisów. Przy projektowaniu należy uwzględnić PN-EN 50131-1:2009 jak również normy i przepisy dotyczące konkretnych pomieszczeń.
4. Projektowany system powinien posiadać GRADE 2.
5. Centralę SSWiN należy zaprojektować (umieścić) w serwerowni.
6. System zaprojektować jako odrębną platformę niezintegrowaną z Systemem Kontroli Dostępu.
7. Instalację przewodową SSWiN należy wykonać przewodem miedzianym np. typu YTDY (ilość żył dobrana stosownie do potrzeb z uwzględnieniem minimum 2 żył zapasowych).
8. System zarządzany będzie przez centralę, do której zostaną podłączone czujki ruchu PIR+MV, kontaktrony magnetyczne z pętlą sabotażową oraz przyciski napadowe. Wszystkie zastosowane urządzenia muszą posiadać wymagane przepisami certyfikaty i spełnić wymagania GRADE 2 (zgodnie z obowiązującymi przepisami i normami oraz regulacjami prawnymi dotyczącymi poszczególnych pomieszczeń).
9. Wszystkie chronione pomieszczenia zabezpieczyć czujnikami PIR+MV (liczbę czujników dobrać do wielkości i kształtu pomieszczenia uwzględniając planowane przeznaczenie pomieszczenia np. regały w pomieszczeniach magazynowych oraz charakterystykę zasięgu torów podczerwieni i mikrofali czujnika), drzwi wejściowe do chronionych pomieszczeń zabezpieczyć kontaktronami, a w przypadku wystąpienia szczególnych przesłanek zastosować kontaktrony i czujniki zbicia szyby do ochrony okien (potrzebę zastosowania czujników zbicia szyby zatwierdza WTI KSP).
10. Do obsługi systemu należy zastosować klawiatury LCD i strefowe oraz moduł łączności TCP IP (ETHM-1 plus) oraz INT-RS.
11. Każde z zabezpieczanych pomieszczeń powinno zostać zaprogramowane jako odrębna strefa i posiadać zainstalowaną klawiaturę strefową oraz sygnalizator akustyczno-optyczny zainstalowane na zewnątrz pomieszczenia. W przypadku lokalizacji kilku chronionych pomieszczeń w niewielkiej odległości od siebie, dopuszczalnym jest zaprojektowanie jednego wspólnego sygnalizatora wewnętrznego akustyczno – optycznego dla danej grupy pomieszczeń.
12. Klawiatury strefowe instalować przy drzwiach wejściowych do pomieszczeń chronionych systemem alarmowym (klawiatura strefowa może obsługiwać tylko jedną strefę), sygnalizator akustyczno-optyczny instalować nad drzwiami pomieszczenia.
13. W przypadku PDOZ zainstalować jeden sygnalizator akustyczno-optyczny na korytarzu.
14. W przypadku projektowania systemu alarmowego dla budynku nie posiadającego 24h służby dyżurnej system alarmowy wyposażyć w zewnętrzny sygnalizator akustyczno-optyczny umiejscowiony na frontowej elewacji budynku (ilość sygnalizatorów dobrana do klasy projektowanego systemu alarmowego).
15. W pomieszczeniu służby dyżurnej zainstalować główną klawiaturę LCD do obsługi całego systemu alarmowego.
16. Wszystkie zastosowane klawiatury LCD i klawiatury strefowe powinny być wyposażone w czytniki kart dostępu.
17. W celu zapewnienia zdalnej obsługi systemu przez program Dloadx, moduł ETHM-1 plus połączyć z płytą centrali dodatkowym przewodem RJ-45 – PIN5.

18. System SSWiN połączyć przewodem sieciowym z Patchpanelem umiejscowionym w szafie z wyjściem sieci LAN do KSP.
19. Do lokalnej obsługi SSWiN programem GuardX, zapewnić możliwość podłączenia komputera w serwerowni za pomocą modułu INT-RS. Dopuszcza się zmianę lokalizacji komputera po konsultacji z użytkownikiem i WTI KSP.
20. Do systemu alarmowego dostarczyć licencję umożliwiającą dodanie i zarządzanie systemem alarmowym z poziomu platformy Integrum.
21. Dostarczana jednostka komputerowa powinna być wyposażona w dodatkowy czytnik kart (USB) kompatybilny z częstotliwościami i rodzajami kart obsługiwanymi przez klawiatury LCD i strefowe projektowanego systemu oraz spełniać wymagania normy Guardx z wgranymi podkładami obiektu i naniesionymi na nie elementami składowymi systemu tj. strefy dozorowe, czujniki, sygnalizatory, przejścia.
22. Zmiana lokalizacji komputera będzie wymuszała zmianę lokalizacji modułu INT-RS (w związku z koniecznością zachowania wymaganych przez producenta odległości okablowania).
23. Do centrali doprowadzić analogową linię telefoniczną.
24. Koniecznym jest zainstalowanie modułu głosowego umożliwiającego przetwarzanie tekstu na mowę (jeśli centrala alarmowa nie jest w takowy wyposażona) wraz z wymaganym okablowaniem oraz dialera telefonicznego (jeśli centrala alarmowa nie jest w takowy wyposażona) umożliwiającego powiadomienie dyżurnego jednostki nadrzędnej o zaistniałym zdarzeniu.
25. System powinien zostać wyposażony w radiolinię z pilotami antynapadowymi (min. 3 szt.)
26. Centralę alarmową zainstalować w serwerowni (lub pomieszczeniu pełniącym jej funkcję), moduły rozszerzeń wejść/ wyjść systemu alarmowego instalować w ciągach komunikacyjnych tuz pod sufitem technicznym.
27. Zastosować akumulatory zasilania awaryjnego SSWIN w oparciu o wykonany bilans energetyczny, pozwalający na zasilanie systemu po odcięciu 230V, zgodnie z wytycznymi dla budowanej klasy systemu.
    Zainstalowane akumulatory powinny być przystosowane do pracy buforowej i powinny posiadać zgodnie z kartą charakterystyki produktu projektową żywotność min. 6 do 9 lat w temp. 20°C.
28. Ponadto pomieszczenia: pokój obsługi interesantów, pokój przesłuchań, pokój okazań, recepcja, magazyny broni, archiwa, kancelarie niejawne, pomieszczenia służby dyżurnej, pomieszczenia dla osób zatrzymanych (na zewnątrz pomieszczenia) – wyposażyć w przyciski napadowe wandaloodporne.
29. Wykonawca zobowiązany jest dostarczyć określoną przez użytkownika liczbę czystych kart/ breloków do obsługi systemu.
30. Wykonawca zobowiązuje się wykonać montaż elementów systemu SSWIN, jego pełną konfigurację (wprowadzenie użytkowników - przypisanie im kart dostępu, określenie stref – w porozumieniu z użytkownikiem, wykonanie logicznych opisów wejść/ wyjść w systemie, pełną konfigurację sieciową), przeprowadzenie testów poprawności działania oraz przeprowadzenie szkolenia z zakresu użytkowania systemu.
31. Zasilanie centrali oraz modułów rozszerzeń wykonać z tablicy TUPS.
32. Systemem SSWiN powinny zostać objęte pomieszczenia (jeżeli są przewidziane w obiekcie):
    - magazyn dowodów rzeczowych
    - archiwum
    - kancelaria niejawna
    - pomieszczenie służby dyżurnej (główny manipulator)

- podręczny magazyn broni,
- magazyn broni,
- magazyn alarmowy
- serwerownia (lub pomieszczenie pełniące jej rolę)
- pomieszczenia ODN
- pomieszczenie Łączności Specjalnej
- PDOZ (przyciski napadowe) – do obsługi tej strefy zainstalować klawiaturę LCD w pomieszczeniu profosa
- lub inne, wskazane przez użytkownika w trakcie wykonywania projektu systemu

Antenowa Instalacja zbiorowa (AIZ)

- Instalację wyposażyć w anteny: satelitarną (fi - 100cm) ustawioną na satelitę Hot Bird 13E, antenę do odbioru cyfrowej telewizji naziemnej w standardzie DVB-T2, anteną radiową w paśmie UKF i FM, antenę radiową do odbioru radia w standardzie DAB+ – wszystkie anteny montować na dachu budynku na dedykowanej do tego celu zwyżce,
- Główny szkielet instalacji antenowej w relacji dach budynku – główny punkt dystrybucyjny projektować w oparciu o włókna światłowodowe (min. 1 włókno w zapasie),
- Wszystkie przewody światłowodowe oznaczyć specjalnymi znacznikami,
- W przypadku rozległych obiektów, w których przewiduje się kilka punktów dystrybucyjnych zbiorczego sygnału telewizyjnego i radiowego szkielet całej sieci między tymi punktami również wykonać w oparciu o włókna światłowodowe (min. 1 włókno w zapasie),
- Wszystkie punkty dystrybucyjne zbiorczego sygnału telewizyjnego i radiowego projektować w ramach możliwości w serwerowniach, w oddzielnych szafkach naściennych przeznaczonych do instalacji tego typu (w innym przypadku lokalizację takiego punktu konsultować na etapie projektu z Wydziałem Teleinformatyki KSP),
- wszystkie szafki instalacji RTV powinny być zasilane z wydzielonego obwodu elektrycznego z oddzielnym zabezpieczeniem w najbliższej rozdzielni elektrycznej,
- Z punktów dystrybucyjnych zbiorczego sygnału telewizyjnego i radiowego, o których mowa w punkcie powyżej sygnał do gniazd abonenckich doprowadzać przewodem koncentrycznym RG – 6 klasy A lub wyższej;
- W każdym projektowanym punkcie dystrybucyjnym zbiorczego sygnału telewizyjnego i radiowego dobrać urządzenia typu multiswitch z uwzględnieniem min. 3 zapasowych wyjść sygnału,
- Gniazda abonenckie powinny być wyposażone w wyjście SAT, Radio, TV naziemna
- W gniazda abonenckie wyposażyć pomieszczenia (jeżeli przewidziano w obiekcie):
    - Pomieszczenie służby dyżurnej
    - Sala odpraw / świetlica
    - Gabinet komendanta, zastępcy komendanta
    - Pomieszczenie rzecznika prasowego
    - Inne (uwzględnić na etapie projektu i skonsultować z użytkownikiem)

System Przyzywowy

Przedmiotem zamówienia jest zakup, dostawa, montaż i konfiguracja kompletnych zestawów przyzywowych w postaci:

1. Panelu głównego sterującego wraz z urządzeniem zasilającym 12V. Panel montowany u Dyżurnego jednostki. Panel powinien obsługiwać określoną przez potrzeby ilość stref (ilość stref zależy od ilości pomieszczeń z przyciskami przyzywanymi). Urządzenie powinno wydawać sygnały dźwiękowe o regulowanej głośności, powinno posiadać podświetlenie/diodę LED (aby zapewnić akustyczną i wizualną sygnalizację alarmu), oraz powinno posiadać przycisk do wyłączenia alarmu. Panel zainstalowany w obudowie podtynkowej lub natynkowej.
2. Panelu podstawowego (przycisku przyzywowego montowanego w pomieszczeniu przejściowym lub PDOZ) wandaloodpornego ze stali nierdzewnej z przyciskiem alarmowym wraz z możliwością resetowania magnetycznego alarmu. Przycisk po wciśnięciu powinien generować sygnał alarmu. Całość w obudowie podtynkowej, zabezpieczona śrubami wandaloodpornymi.

Dodatkowe wymagania:

1. Instalacja wewnątrz celi nie może być prowadzona metodą na tynkową,
2. Przycisk w celi musi być zamontowany w sposób uniemożliwiający demontaż przez osobę zatrzymaną,
3. Przycisk w celi nie może posiadać ostrych krawędzi umożliwiających samookaleczenie,
4. Instalacja przyzywowa musi posiadać bezpieczne napięcie 12-24V DC,
5. Włącznik alarmu przyzywowego powinien sygnalizować ledem/podświetleniem poprawność działania przycisku,
6. Sygnalizator może być zintegrowany z przyciskiem na jednym panelu lub zamontowany oddzielnie w miejscu widocznym dla osadzonego w sposób uniemożliwiający dewastację,
7. Długie i częste przytrzymywanie włącznika nie może powodować przeciążenia układu,
8. W ramach instalacji należy wykonać przycisk kasowania alarmu w wyznaczonym przez osobę nadzorującą miejscu, kasujący alarm dźwiękowy i świetlny,
9. Przycisk kasowania odporny na długotrwałe wciśnięcie lub zablokowanie przycisku – przy długotrwałym przyciśnięciu nie blokujący następnego alarmu,
10. System ma posiadać własny rejestrator alarmów rejestrujący wszystkie występujące alarmy.

Urządzenia aktywne

Brama Głosowa

Wyposażenie

1. Urządzenie musi być routerem modularnym wyposażonym w minimum 4 interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połączenia do sieci WAN. Interfejsy te muszą mieć

możliwość pracy w trybie „dual-physical" z gigabitowymi portami światłowodowymi definiowanymi przez SFP.

2. Urządzenie musi być wyposażone w minimum dwa porty USB. Porty muszą pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych oraz pełnić funkcję konsoli szeregowej.
3. Musi być wyposażone w co najmniej 4 portów FXS do realizacji usług głosowych.
4. Musi być wyposażone w co najmniej 4 porty BRI do realizacji usług głosowych.
5. Urządzenie musi być wyposażone w minimum 25 licencji użytkowników na SRST.

Architektura

6. Musi być urządzeniem modularnym posiadającym możliwość instalacji, co najmniej 3 modułów sieciowych z interfejsami.
7. Musi posiadać możliwość wyposażenia w co najmniej 8 portów FXS do realizacji usług głosowych.
8. Musi posiadać możliwość wyposażenia w co najmniej 4 porty BRI do realizacji usług głosowych.
9. Musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Np. niedopuszczalne jest stosowanie karty 4-portowej gdzie aktywne są 2 porty, a dla uruchomienia pozostałych konieczne jest wpisanie kodu, który uzyskuje się przez wykupienie licencji na użytkowanie pozostałych portów.
10. Sloty urządzenia przewidziane pod rozbudowę muszą mieć możliwość obsadzenia modułami:
    a. z portami szeregowymi - o gęstości co najmniej 4 porty na moduł,
    b. z interfejsem ISDN BRI (styk S/T) - o gęstości co najmniej 4 portów na moduł,
    c. z przełącznikiem Ethernet - o gęstości co najmniej 8 portów na moduł,
11. Oczekiwana wydajność proponowanego rozwiązania z włączonymi usługami nie może być mniejsza niż 500Mbit/s zarówno dla ruchu nieszyfrowanego jak i szyfrowanego.

Oprogramowanie - funkcjonalność

12. Oprogramowanie routera musi umożliwiać rozbudowę o dodatkowe funkcjonalności bez konieczności instalacji nowego oprogramowania. Nowe zbiory funkcjonalności muszą być dostępne poprzez wprowadzenie odpowiednich licencji.
13. Musi posiadać obsługę protokołów routingu IP BGPv4, OSPF, IS-IS, RIPv2 oraz routingu multicastowego PIM (Sparse i Dense) oraz routing statyczny.
14. Protokół BGP musi posiadać obsługę 4 bajtowych ASN.
15. Musi posiadać wsparcie dla funkcjonalności Policy Based Routing.
16. Musi posiadać wsparcie dla mechanizmów związanych z obsługą ruchu multicast: IGMPv3, IGMP Snooping, PIMvl, PIMv2.
17. Musi posiadać wsparcie dla protokołu DVMRP.
18. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF).
19. Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q.
20. Musi obsługiwać IPv6 w tym ICMP dla IPv6.
21. Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL.
22. Musi zapewniać mechanizmy korelacji zdarzeń związanych z filtracją za pomocą list kontroli dostępu dla syslog (np. za pomocą etykiety przypisanej do określonego wpisu na listach kontroli dostępu lub skrót MD5 generowany przez router).

23. Musi posiadać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.
24. Mechanizm NAT musi zapewniać wsparcie dla H.224/H.245.
25. Musi posiadać wsparcie dla protokołów WCCP i WCCPv2.
26. Musi posiadać obsługę mechanizmu DiffServ.
27. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu.
28. Musi zapewniać obsługę mechanizmów kolejkowania ruchu:
    a. z obsługą kolejki absolutnego priorytetu,
    b. ze statyczną alokacją pasma dla typu ruchu,
    c. WFQ.
29. Musi obsługiwać mechanizm WRED.
30. Musi obsługiwać protokół RSVP.
31. Musi obsługiwać mechanizm Generic Traffic Shaping.
32. Musi obsługiwać mechanizm ograniczania pasma dla określonego typu ruchu.
33. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego.
34. Musi obsługiwać protokół NTP.
35. Musi obsługiwać DHCP w zakresie Client, Server.
36. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika).
37. Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+.
38. Musi posiadać możliwość współpracy z centralnym systemem procesowania połączeń telefonii IP w celu przejęcia podstawowych funkcji telefonii do połączeń wewnętrznych oraz wyjścia na linie miejskie na czas awarii połączenia do systemu centralnego. Funkcja ta musi być w stanie obsłużyć co najmniej 64 abonentów.
39. Musi posiadać funkcje pozwalające na automatyzację konfiguracji ustawień QoS (w szczególności dla usług VoIP) w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS.
40. Musi posiadać funkcjonalność sondy (nadajnik i odbiornik) do mierzenia parametrów ruchu dla protokołów IP oraz VoIP (pomiar jakości poprzez symulację kodeków VoIP i mierzenie parametrów opóźnienia „tam i z powrotem" (round trip), jitter i utraty pakietów).
41. Musi posiadać funkcjonalność firewall (w trybie routed oraz transparent).
42. Musi posiadać funkcjonalność Intrusion Prevention System.
43. Musi posiadać funkcjonalność Content Filtering.
44. Musi posiadać możliwość szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES, w tym beztunelowego szyfrowania w oparciu o zarządzanie kluczami wg algorytmu GDOI zgodnie
    z RFC 3547.

Zarządzanie i konfiguracja

45. Musi być zarządzany za pomocą SSHv2, SNMPv2, SNMPv3.
46. Musi być kompatybilne z Cisco Unified Communications Manager w ver. 12.5.1 posiadaną przez Zamawiającego oraz z wersjami nowszymi.
47. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu Netflow/JFlow lub odpowiednika.
48. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface - CLI).
49. Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian

konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

Obudowa

50. Musi być wykonana z metalu. Ze względu na różne warunki w których pracować będą urządzenia, nie dopuszcza się stosowania urządzeń w obudowie plastikowej.
51. Musi mieć możliwość montażu w szafie 19".

Zasilanie

52. Urządzenie musi mieć możliwość zasilania ze źródeł zmiennoprądowych 230V (zasilacza AC) oraz stałoprądowych (zasilacze DC).
53. Urządzenie musi posiadać 2 wbudowane zasilacze umożliwiające zasilanie prądem przemiennym 230V.
54. Urządzenie musi umożliwiać doprowadzenie zasilania do portów Ethernet (tzw. inline-power) - w modułach sieciowych dostępnych do urządzenia.

Serwis

55. Dostarczany sprzęt musi być objęty min. 36-miesięcznym (3 lata) serwisem opartym na serwisie producenta urządzenia świadczonym w reżimie 8x5xNBD.

Rejestrator korespondencji radiowo-telefonicznej.

Nowo budowany obiekt należy wyposażyć w rejestrator korespondencji radiowo-telefonicznej. Rejestrator jest wymagany jeżeli w jednostce jest stanowisko służby dyżurnej lub stanowisko sztabowe.

Minimalne parametry techniczne i wymagania funkcjonalne urządzenia:

Wymagania techniczne

1. Urządzenie powinno mieć zdolność rejestracji min. 32 kanałów,
2. Praca pod nadzorem systemu operacyjnego o wielkości do 500 MB zainstalowanego na wymiennym flash dysku. (możliwość zdalnej aktualizacji i zmiany wersji systemu operacyjnego przez wgranie pojedynczego pliku),
3. Skalowalny system operacyjny pozbawiony zbędnych komponentów, zawierający wyłącznie funkcje wykorzystywane przez rejestrator,
4. Posiadać interfejs umożliwiający rejestracje 4 linii analogowych faks-telefonicznych z FSK i DTMF,
5. Posiadać interfejs umożliwiający rejestracje 4 aparatów systemowych (np. Panasonic, DGT, Siemens) lub 2 ISDN (BRA 2B+D),
6. Posiadać interfejs do rejestracji kanałów VoIP – min. 4 terminali,
7. Posiadać interfejs do rejestracji kanałów IP z systemów dyspozytorskich TRX i Multikom2 – min 4 kanały,
8. Możliwość integracji z systemami dyspozytorskimi TRX i Multikom2,
9. Zarządzanie rejestratorem – lokalne i zdalne (sieć LAN, protokół TCP/IP),
10. Posiadać interfejs współpracy z zewnętrzna pamięcią masową,

11. Niezależne dyski do zapisu treści rozmów.

Realizowane funkcje rejestratora rozmów:

1. Automatyczne przygotowanie nowego dysku do nagrywania rozmów,
2. Rejestracja rozmów abonentów telefonów systemowych (np. Panasonic, DGT, Siemens, itp.) oraz ISDN (BRA 2B+D), zmiana na konkretny model ma następować poprzez wgranie odpowiedniego oprogramowania karty,
3. Rejestracji kanałów VoIP (platforma głosowa CUCM wer.8.6.2.21900-5 i wyższe) z sygnalizacjami SIP, H.323,
4. Rejestracja korespondencji prowadzonej na platformach dyspozytorskich Multikom2 lub TRX,
5. Wbudowana przestrzeń dyskowa umożliwiająca zapis min. 30 tys. godzin rozmów,
6. Zdalne powiadamianie o zdarzeniach w funkcjonowaniu i awariach rejestratora (uszkodzenie dysku, odłączenie połączenia Ethernet),
7. Zapis informacji o numerze telefonu wywoływanego i wywołującego z linii cyfrowych, systemowych i analogowych również w przypadku połączeń nieodebranych (czasy oczekiwania na połączenie),
8. Zapis daty i czasu połączenia, czasu trwania rozmowy,
9. Różne kryteria rozpoczęcia rejestracji rozmowy: poziom głosu VOX, sygnalizacją, po sygnale dzwonienia, rejestracja ciągła, RTP (VoIP),
10. Dekodowanie sygnalizacji DTMF,
11. Niezależne nagrywanie każdego kanału,
12. Lokalny i zdalny podgląd i podsłuch wszystkich nagrywanych portów w czasie rzeczywistym, jedną aplikacją,
13. Automatyczna i ręczna regulacja wzmocnienia nagrywania kanałów, dopuszczone AGC off-line,
14. Odsłuch rozmowy niezależnie od jej rejestracji w danym czasie,
15. Zintegrowany głośnik,
16. Wyświetlacz LCD (informacja o aktualnym stanie urządzenia),
17. Klawisze funkcyjne umożliwiające lokalne podstawowe zarządzanie rejestratorem i odsłuch,
18. Sygnalizacja świetlna stanu portu na urządzeniu po podłączeniu linii (synchronizacja lub jej brak dla linii systemowych i ISDN).

Funkcje archiwizacji:

1. Identyfikacja i archiwizacja nagrań w bazie danych z nim skojarzonych, co najmniej: data, czas trwania, numer abonentów A i B, rodzaj kompresji, komentarz,
2. Identyfikacja i archiwizacja nagrań abonenta VoIP w bazie danych z nim skojarzonych, co najmniej: data, czas trwania, numer strony A i B, adres MAC, adres IP, komentarz,
3. Możliwość wyszukiwania nagrania po danych z nim skojarzonych,
4. Możliwość automatycznej archiwizacji nagrań i danych z nimi skojarzonych w systemie zewnętrznej pamięci masowej,
5. Dostęp do bazy danych (archiwum nagrań) w systemie zewnętrznej pamięci masowej z poziomu oprogramowania zarządzającego rejestratorem,

6. Możliwość wykonania archiwizacji nagrań na nośnikach wymiennych w formacie pliku mp3 lub wave,
7. Automatyczne kasowanie najstarszych nagrań po zapełnieniu się dysku,
8. Mirror dysków z funkcją wymiany i odbudowy bez przerw w nagrywaniu,
9. Musi posiadać możliwość zainstalowania i uruchomienia oprogramowania do wizualizacji faksów.

Funkcje zarządzania i zabezpieczeń:

1. Lokalne i zdalne zarządzanie rejestratorem w sieci LAN (protokół TCP/IP),
2. Szybkie automatyczne przywrócenie działania po zaniku zasilania,
3. Bezobsługowa baza danych nie wymagająca okresowych czynności użytkownika, odporna na niekontrolowane zaniki zasilania,
4. Program do zdalnego monitorowania i sygnalizacji poprawnej pracy rejestratora, w tym: automatyczna sygnalizacja utraty połączenia i innych nieprawidłowych stanów (np. zwarcie, zbyt długa rozmowa, dla nagrywanych źródeł: linie analogowe, cyfrowe i VoIP,
5. Wielopoziomowy system zabezpieczeń, praw dostępu i uprawnień do zarejestrowanych nagrań: konfiguracja, podsłuch/odsłuch, archiwizacja,
6. Oprogramowanie do zarządzania i odsłuchu bez ograniczenia liczby stanowisk,
7. Możliwość rekonfiguracji poszczególnych kanałów w trakcie pracy systemu bez konieczności jego resetu,
8. Możliwość odsłuchiwania zarejestrowanych rozmów w trakcie dokonywania nagrań, lokalnie i zdalnie przez sieć Ethernet na standardowym PC z kartą dźwiękową z poziomu dedykowanej aplikacji jak również przez Web-interface (przeglądarka),
9. Brak możliwości wykasowania pojedynczych rozmów i jakiejkolwiek modyfikacji plików zawierających treść nagranych korespondencji, bez względu na uprawnienia
10. Podgląd stanu portu,
11. Bezpłatny upgrade oprogramowania włącznie z systemem operacyjnym rejestratora (możliwość zdalnego wykonania tej czynności przez administratora systemu).

Warunki pracy rejestratora:

1. Zasilanie – 230 V,
2. Obudowa umożliwiająca montaż w szafie 19" max. 3U.

Switche Corowe

Cisco C9300-48S-A lub Cisco C9300-24S-A (minimum 2 szt.) - (oprogramowanie Advantage) lub inny o parametrach i funkcjonalnościach nie gorszych niż niżej wymienione:

Dla C9300-48S-A:
- 48 porty 1G SFP
- 1 slot na moduł rozszerzeń obsadzony modułem 8x10G SFP+
- Zamiennik modułu/wkładki SFP+ Cisco SFP-10G-LR – 10 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-D43 - 48 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-U34 - 48 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-TE/GLC-T/SFP-GE-T - 24 szt.

Dla C9300-24S-A:

- 24 porty 1G SFP
- 1 slot na moduł rozszerzeń obsadzony modułem 8x10G SFP+
- Zamiennik modułu/wkładki SFP+ Cisco SFP-10G-LR - 10 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-D43 - 24 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-U34 - 24 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-TE/GLC-T/SFP-GE-T - 24 szt.

Parametry i funkcjonalności wspólne dla wyżej wymienionych urządzeń:

1. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco" – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
   - 4x1G SFP
   - 8x1/10G SFP+
   - 2x40G QSFP
   - 4x100M/1G/2.5G/5G/10GBaseT RJ-45
   - 2x25G SFP28
2. Możliwość łączenia w stos z zapewnieniem następujących funkcjonalności:
   - Przepustowość w ramach stosu - 480Gb/s
   - 8 urządzeń w stosie
   - Zarządzanie poprzez jeden adres IP
   - Możliwość tworzenia połączeń cross-stack Link Aggregation zgodnie z IEEE 802.3ad
   - Możliwość współdzielenia mocy zasilaczy dla grup liczących 4 przełączniki - tzn. zasilacze stanowią zasób wspólny dla wszystkich przełączników w grupie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie)
   - Urządzenie musi być dostarczone z zestawem przewodów umożliwiających stackowanie (przewód stackujący o dł. 0.5m oraz przewód stackujący zasilanie o dł. 0.3).
3. Parametry fizyczne
   - Urządzenia wyposażone w 2 wymienne, redundantne zasilacze AC 230V
   - Możliwość instalacji zasilacza prądu stałego, jak również jednoczesnej instalacji zasilacza prądu zmiennego i stałego
   - Urządzenie wyposażone w redundantne i wymienne moduły wentylatorów
   - Wysokość przełącznika 1RU
   - Możliwość montażu w szafie 19".
4. Obsługa IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności).
5. Inteligentne funkcje dla POE:
   - Perpetual PoE – podtrzymywanie zasilania dla krytycznych urządzeń podczas restartu przełącznika (np. kamery IP)
   - Fast POE - po przywróceniu zasilania przełącznik zaczyna dostarczać moc do punktów końcowych bez czekania na pełne załadowanie systemu operacyjnego przełącznika, co przyspiesza uruchomienie podłączonego urządzenia.
6. Parametry wydajnościowe:
   - Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
   - Bufor pakietów – nie mniej niż 16MB
   - Pamięć DRAM – 8GB

- Pamięć flash – 16GB
- Obsługa
  - 4.000 sieci VLAN
  - 32.000 adresów MAC
  - 32.000 tras IPv4
  - 16.000 tras IPv6.

7. Obsługa protokołu NTP.
8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
   - IEEE 802.1w Rapid Spanning Tree
   - Per-VLAN Rapid Spanning Tree (PVRST+)
   - IEEE 802.1s Multi-Instance Spanning Tree
   - Obsługa 128 instancji protokołu STP
10. Obsługa protokołu CDP, LLDP i LLDP-MED.
11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
12. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
13. Mechanizmy związane z bezpieczeństwem sieci:
    - Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level).
    - Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością:
      - dynamicznego przypisania użytkownika do określonej sieci VLAN
      - dynamicznego przypisania listy ACL.
    - Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.
    - Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www).
    - Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    - 5000 wpisów dla list kontroli dostępu (Security ACE).
    - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).
    - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
    - Obsługa list kontroli dostępu (ACL).
    - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128).

- Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing).
- Funkcja Private VLAN.

14. Zestaw narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych obejmujące:
    - podpisywanie cyfrowe i weryfikację podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.) – tzw. Image signing.
    - wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu i jego jednoznaczną identyfikację – Trust Anchor Module.
    - bezpieczne uruchamianie (secure boot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiające uruchomienie nielegalnie zmodyfikowanego oprogramowania systemowego.
15. Możliwość uruchomienia funkcji serwera DHCP.
16. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    - Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    - Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting).
    - Kontrola sztormów dla ruchu broadcast/multicast/unicast.
    - Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
17. Obsługa protokołów routingu:
    - Routing statyczny dla IPv4 i IPv6.
    - Routing dynamiczny IPv4/IPv6 – RIP, OSPF (1000 tras), EIGRP Stub.
    - Policy-based routing (PBR).
    - Obsługa protokołu redundancji bramy – VRRP.
18. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN.
19. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
20. Zarządzanie
    - Port konsoli.
    - Dedykowany port Ethernet do zarządzania out-of-band.
    - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    - Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
    - Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.

- Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów.
- Obsługa protokołu gRPC Dial-Out.
- Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
- Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
- Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku.

Dodatkowe funkcje i możliwości dla przełączników z oprogramowaniem Advantage

21. Mechanizmy związane z bezpieczeństwem sieci:
    - Możliwość przypisywania w ramach uwierzytelniania i autoryzacji 802.1X specjalnych identyfikatorów (znaczniki SGT), które mogą zostać wykorzystane do budowy polityk bezpieczeństwa niezależnych od topologii fizycznej i logicznej sieci (bez konieczności wykorzystywania informacji o VLANach i adresach IP). Przełącznik ma możliwość bezpośredniego egzekwowania polityki bezpieczeństwa, jak również przenoszenia informacji o identyfikatorze danego użytkownika/urządzenia przez sieć do innych urządzeń.
    - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) kluczami o długości 256-bitów (gcm-aes-256).
22. Wsparcie dla protokołu LISP zgodnie z RFC 6830.
23. Obsługa MPLS – w tym L3 VPN, Multicast VPN (mVPN), EoMPLS, VPLS.
24. Obsługa zaawansowanych protokołów routingu:
    - IS-IS i BGP dla IPv4 i IPv6
    - EIGRP
    - Routing multicastów - PIM-SM, PIM-SSM
    - Multicast Source Discovery Protocol (MSDP)
    - VRF-Lite.
25. Możliwość enkapsulacji ruchu w pakiety VXLAN.
26. Obsługa standardu IEEE 802.1 AVB (Audio Video Bridging).
27. Precision Time Protocol (PTP; IEEE 1588v2).

Dodatkowe możliwości przełączników (usługi subskrypcyjne)

28. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 64.000 strumieni.
29. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.

Dodatkowe funkcje i możliwości dla przełączników z oprogramowaniem Advantage(usługi subskrypcyjne)

30. Funkcjonalność bramy dla usług mDNS.
31. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN).
32. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7).

33. Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Packekt) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).
34. Wbudowany analizator pakietów.
35. Możliwość obsługi dodatkowych aplikacji na przełączniku (w kontenerach/VMkach).

Dodatkowe wymagania formalne:

1. Zamawiający wymaga aby miał pełne prawa do korzystania z licencji i oprogramowania zainstalowanego w urządzeniach.

2. Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe były fabrycznie nowe i na dzień składania ofert niewycofane przez producenta ze sprzedaży.

3. Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe pochodziły z oficjalnego kanału dystrybucyjnego producenta urządzeń na rynek polski.

4. Zamawiający wymaga aby dostarczony sprzęt był zarejestrowany na Komendę Stołeczną Policji w Warszawie lub jednostkę nadrzędną w celu posiadania pełnych praw licencyjnych i gwarancyjnych.

5. Zamawiający wymaga aby wszystkie dostarczane urządzenia posiadały cechy/atrybuty ich legalności, tj. oznaczenie producenta, modelu oraz numeru seryjnego urządzenia.

6. Zmawiający wymaga aby Wykonawca przed dostawą dostarczył numery seryjne urządzeń celem weryfikacji źródła ich pochodzenia u producenta. W przypadku negatywnej weryfikacji, Zamawiający może odmówić przyjęcia urządzeń.

Switche Dystrybucyjne

Cisco C9200L-48P-4G-E (ilość zależna od ilości oraz rozkładu PEL) lub inny o parametrach i funkcjonalnościach nie gorszych niż niżej wymienione:

- 48 portów 10/100/1000 RJ45 PoE+ (zgodne z IEEE 802.3at)
- 4 porty uplinkGigabit Ethernet SFP
- Moc dostępna dla portów PoE/PoE+ wynosząca 740W
- PSU PWR-C5-1KWAC - 1 szt.
- STACK-KIT C9200L-STACK-KIT – 1 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-D43 - 2 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-BX20-U34 - 2 szt.
- Zamiennik modułu/wkładki SFP Cisco GLC-TE/GLC-T/SFP-GE-T - 4 szt.

Parametry i funkcjonalności:

1. Parametry fizyczne:
    - Urządzenia wyposażone w 2 wymienne, redundantne zasilacze AC 230V.

- Dla urządzeń z portami PoE+ wyposażonych w dwa zasilacze możliwość dostarczenia mocy 30W dla każdego z dostępnych portów PoE+.
- Urządzenie wyposażone w redundantne moduły wentylatorów z możliwością pracy przy awarii jednego z nich.
- Wysokość przełącznika 1RU.
- Możliwość montażu w szafie 19".

2. Możliwość rozszerzenia funkcjonalności przełącznika o funkcję stackowania z zapewnieniem następujących funkcjonalności:
   - Przepustowość w ramach stosu –80Gb/s.
   - 8 urządzeń w stosie.
   - Zarządzanie poprzez jeden adres IP.
   - Możliwość tworzenia połączeń cross-stack Link Aggregation zgodnie z IEEE 802.3ad.
   - Stackowanie z wykorzystaniem opcjonalnego dedykowanego modułu – bez ograniczania liczby dostępnych portów uplink.
3. Obsługa IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności).
4. Inteligentne funkcje dla POE:
   - Perpetual PoE – podtrzymywanie zasilania dla krytycznych urządzeń podczas restartu przełącznika (np. kamery IP).
   - Fast PoE - po przywróceniu zasilania przełącznik zaczyna dostarczać moc do punktów końcowych bez czekania na pełne załadowanie systemu operacyjnego przełącznika, co przyspiesza uruchomienie podłączonego urządzenia.
5. Parametry wydajnościowe:
   - Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów (przełącznik line-rate).
   - Bufor pakietów – 6MB.
   - Pamięć DRAM – 2GB; pamięć flash – 4GB.
   - Obsługa:
     i. 1024 sieci VLAN,
     ii. 512 interfejsów SVI,
     iii. 16.000 adresów MAC,
     iv. 3.000 tras IPv4,
     v. 1.500 tras IPv6.
6. Obsługa protokołu NTP.
7. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
8. Wsparcie następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
   - IEEE 802.1w Rapid Spanning Tree,
   - IEEE 802.1s Multi-Instance Spanning Tree,
   - Per-VLAN Rapid Spanning Tree (PVRST+),
   - Obsługa128 instancji protokołu STP.
9. Obsługa protokołów CDP, LLDP i LLDP-MED.
10. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
12. Mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level).
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością:
  i. dynamicznego przypisania użytkownika do określonej sieci VLAN,
  ii. dynamicznego przypisania listy ACL.
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
- Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.
- Funkcjonalność flexibleauthentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www).
- Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
- 1500 wpisów dla list kontroli dostępu (Security ACE).
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
- Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
- Obsługa list kontroli dostępu (ACL).
- Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128).
- Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control PlanePolicing).
- Funkcja Private VLAN.

13. Zestaw narzędzi pozwalających na kontrolę pochodzenia przełączników i działającego na nich oprogramowania oraz wykluczenie możliwości ich modyfikacji podczas procesów produkcyjnych lub logistycznych obejmujące:
    - podpisywanie cyfrowe i weryfikację podpisu wszystkich komponentów programowych przełącznika (BIOS, firmware itp.) – tzw. Image signing,
    - wyposażenie przełączników w bezpieczne, odporne na manipulacje układy kryptograficzne, gwarantujące uwierzytelnienie oryginalności sprzętu i jego jednoznaczną identyfikację – Trust Anchor Module,
    - bezpieczne uruchamianie (secureboot), zapewniające sprzętową weryfikację sekwencji startowej i uniemożliwiające uruchomienie nielegalnie zmodyfikowanego oprogramowania systemowego.
14. Możliwość uruchomienia funkcji serwera DHCP.
15. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    - Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    - Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (StrictPriority),

- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, ratelimiting),
- Kontrola sztormów dla ruchu broadcast/multicast/unknownunicast,
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

16. Obsługa protokołów routingu:
    - Routing statyczny dla IPv4 i IPv6,
    - Routing dynamiczny IPv4/IPv6 – RIP, OSPF (1000 tras), EIGRP Stub,
    - Policy-based routing (PBR),
    - Obsługa protokołu redundancji bramy –VRRP.
17. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN.
18. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
19. Zarządzanie:
    - Port konsoli.
    - Dedykowany port Ethernet do zarządzania out-of-band.
    - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    - Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
    - Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.
    - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów.
    - Obsługa protokołu gRPCDial-Out.
    - Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
    - Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
20. Możliwość rozszerzenia funkcjonalności (za pomocą dodatkowych licencji bez konieczności modyfikacji sprzętowych) o obsługę następujących funkcji:
    - Możliwość przypisywania w ramach uwierzytelniania i autoryzacji 802.1X specjalnych identyfikatorów (znaczniki SGT), które mogą zostać wykorzystane do budowy polityk bezpieczeństwa niezależnych od topologii fizycznej i logicznej sieci (bez konieczności wykorzystywania informacji o VLANach i adresach IP). Przełącznik ma możliwość bezpośredniego egzekwowania polityki bezpieczeństwa, jak również przenoszenia informacji o identyfikatorze danego użytkownika/urządzenia przez sieć do innych urządzeń.
    - Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 16.000 strumieni.

- Obsługa protokołu redundancji bramy – HSRP.
- Obsługa zaawansowanych protokołów routingu dla IPv4 i IPv6 – IS-IS.
- Routing multicastów - PIM-SM, PIM-SSM.
- Multicast Source Discovery Protocol (MSDP).
- Obsługaprotokołu LISP (Locator/ID Separation Protocol)orazenkapsulacji VXLAN.
- Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.

Dodatkowe wymagania formalne:

1. Zamawiający wymaga aby miał pełne prawa do korzystania z licencji i oprogramowania zainstalowanego w urządzeniach.

2. Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe były fabrycznie nowe i na dzień składania ofert niewycofane przez producenta ze sprzedaży.

3. Zamawiający wymaga aby dostarczane urządzenia, a także ich wyposażenie i akcesoria montażowe pochodziły z oficjalnego kanału dystrybucyjnego producenta urządzeń na rynek polski.

4. Zamawiający wymaga aby dostarczony sprzęt był zarejestrowany na Komendę Stołeczną Policji w Warszawie lub jednostkę nadrzędną w celu posiadania pełnych praw licencyjnych i gwarancyjnych.

5. Zamawiający wymaga aby wszystkie dostarczane urządzenia posiadały cechy/atrybuty ich legalności, tj. oznaczenie producenta, modelu oraz numeru seryjnego urządzenia.

6. Zmawiający wymaga aby Wykonawca przed dostawą dostarczył numery seryjne urządzeń celem weryfikacji źródła ich pochodzenia u producenta. W przypadku negatywnej weryfikacji, Zamawiający może odmówić przyjęcia urządzeń.

Policyjny System Wideokonferencyjny

Policyjny System Wideokonferencyjny jest projektem procedowanym przez Biuro Łączności i Informatyki Komendy Głównej Policji, który w swoich założeniach polega na doposażeniu wszystkich jednostek poziomu Komend Rejonowych, Powiatowych Policji oraz wybranych wydziałów w zestaw wideokonferencyjny. System ten jest wewnętrzną platformą komunikacji multimedialnej opartą na własnej infrastrukturze serwerowej i terminalach wideokonferencyjnych funkcjonujących w dedykowanej podsieci IP, wydzielonej w ramach infrastruktury OST 112.

System wideokonferencyjny umożliwia prowadzenie wideorozmów między wszystkimi użytkownikami wyposażonymi w podobny system. Komenda Stołeczna Policji zyska dzięki temu wszechstronne i bezpieczne rozwiązanie pozwalające na prowadzenie odpraw służbowych, szkoleń lub zebrań celem zwiększenia efektywności codziennej pracy.

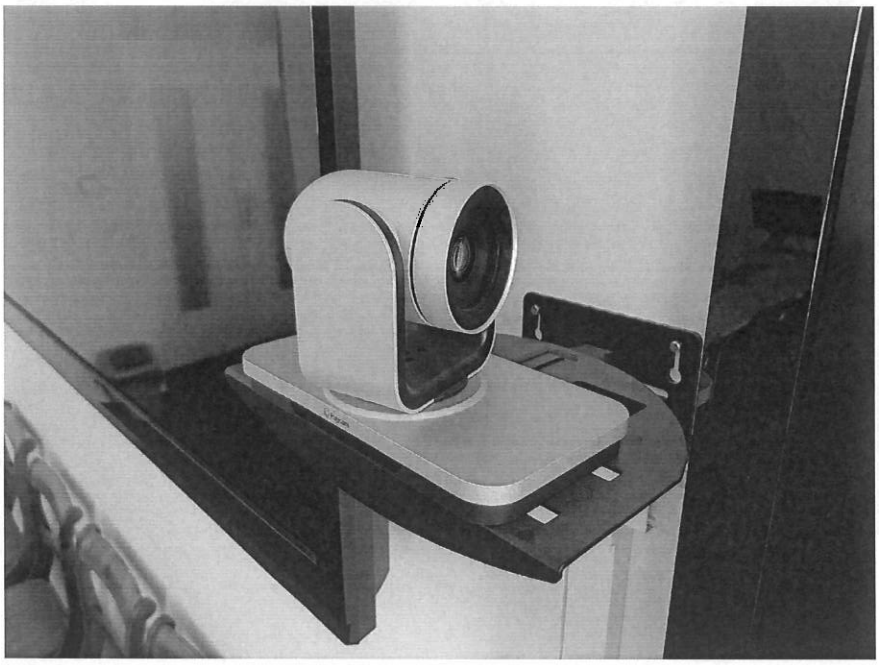
Pomieszczenie, w którym mają się odbywać wideokonferencje powinno zostać odpowiednio przystosowane ze względu na wymagania techniczne jak i wizualne.

Wymagania techniczno-organizacyjne PSW

1, Wymagania techniczne

- Zasilanie

Urządzenia wideokonferencyjne są zasilane prądem zmiennym 230V z sieci. Jednakże optyka urządzenia pracujące w kamerze urządzenia jest poruszana specjalnym elektromagnetycznym mechanizmem, które w przypadku nagłego zerwania zasilania może zostać uszkodzone, dlatego zalecanym jest, aby sam terminal wideokonferencyjny był zasilany z sieci zasilania gwarantowanego danej jednostki/komórki organizacyjnej Policji (ok 300 watów).



fot. mechanizmu optyki kamery)

- Komunikacja sieciowa urządzenia wideokonferencyjnego.

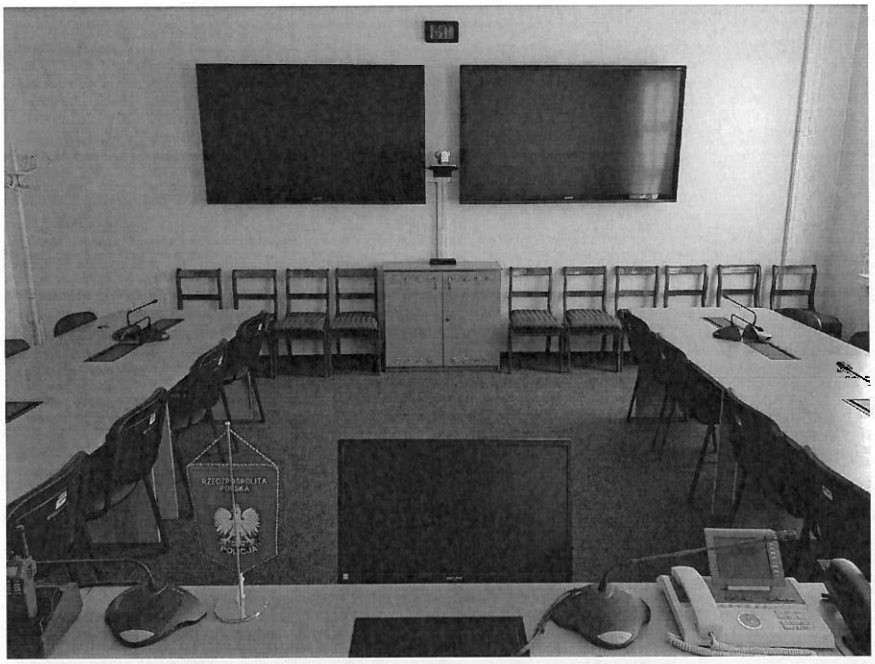
Urządzenia wideokonferencyjne wymagają podłączenia do sieci LAN za pomocą standardowego sieciowego wtyku RJ45.

Terminale wideokonferencyjne pracują w sieci PSTD. Należy przeznaczyć jedno wolne miejsce w switchu PSTD danej jednostki/komórki organizacyjnej na pracę wideoterminala.

Terminal wideokonferencyjny jest urządzeniem, które bardzo rozsądnie skaluje możliwości przesyłania danych po sieci i potrafi zapewnić dobrej jakości połączenie wideo i audio już przy zapewnieniu łącza 512 kb/s.

- Wyświetlanie obrazu wideokonferencyjnego

System Wideokonferencyjny pozwala na jednoczesne wyświetlanie kilku obrazów konferencyjnych na jednym lub wielu ekranach. Obecne założenia systemu zakładają, że każda komórka/jednostka organizacyjna Komendy Stołecznej Policji wyznaczona do PSW zostanie doposażona w minimum jeden duży monitor do wyświetlania wideokonferencji. W zależności od wielkości i możliwości technicznych pomieszczenia przeznaczonego do prowadzenia wideokonferencji.



(fot. przedstawiające istniejące rozwiązanie wideokonferencyjne wyposażone w dwa ekrany na stałe przymocowane do ściany)

2. Wymagania organizacyjne

- Logotyp jednostki

W trakcie prowadzenia wideokonferencji, komfort uczestników wideokonferencji znacznie zwiększa istnienie napisu przedstawiającego logotyp danej jednostki/komórki organizacyjnej KSP tuż za plecami uczestników spotkania.

Wydział Inwestycji i Remontów KSP aktualnie prowadzi prace mające na celu doposażenie jednostek Policji w napis informujący o jednostce/komórce organizacyjnej.

- Oświetlenie

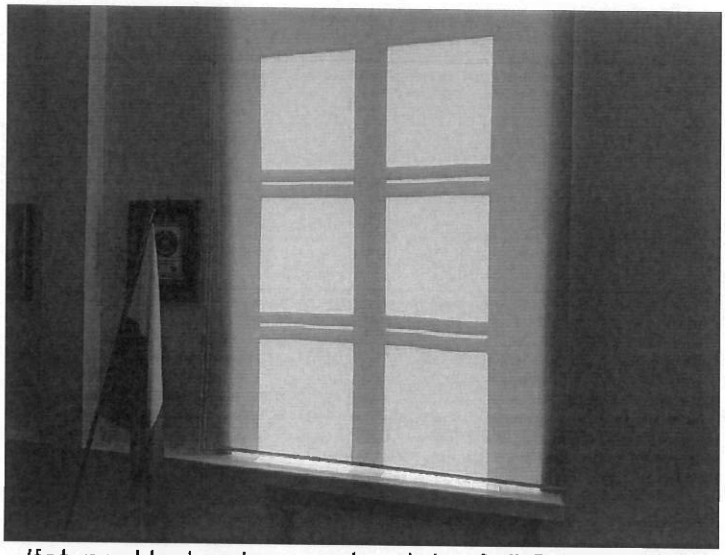
Aby uczestnik wideokonferencji mógł być dobrze widziany dla innych uczestników spotkania, musi być dobrze oświetlony. Pomieszczenie powinno rzucać światło min. 300 luksów, żeby zapewnić odpowiedni kontrast. Podczas dostosowywania oświetlenia należy wziąć pod uwagę jak największe rozproszenie światła, dzięki czemu uczestnicy rzucają mniejsze cienie.

Oświetlenie też powinno zostać zainstalowane w torze między kamerą systemu a uczestnikiem wideokonferencji, ale tuż przed uczestnikiem. Światło zainstalowane bezpośrednio nad głową osoby biorącej udział w konferencji może spowodować niekorzystne światłocienie dla pozostałych uczestników spotkania.

(fot. Ramy oświetlenia odbijają światło od dołu powodując rozproszenie światła)

- Zasłony

Pomieszczenie przeznaczone do systemu wideokonferencyjnego powinno posiadać działające rolety, żaluzje lub w inny sposób zapewniać dyskrecję dla uczestników wideokonferencji od zewnątrz.



(fot. przykład zastosowanie rolet w Sali Generalskiej KSP)

- Klimatyzacja

Celem zapewnienia prawidłowych warunków środowiskowych dla zaawansowanych urządzeń telekomunikacyjnych oraz celem zapewnienie komfortu dla samych uczestników wideokonferencji, pomieszczenie przeznaczone do systemu wideokonferencyjnego powinno być wyposażone w działającą klimatyzację.

- Wielkość i lokalizacja pomieszczenia

Pomieszczenie przeznaczone do systemu wideokonferencyjnego powinno być oddzielnym wyznaczonym pomieszczeniem tylko do tego typu spotkań lub w sali odpraw w danej jednostce/komórce organizacyjnej KSP. W miarę możliwości, pomieszczenie powinno być oddalone od głównych ciągów komunikacyjnych jednostki oraz wygłuszone oraz wyciszone. Z uwagi na wielofunkcyjność systemu, pomieszczeniem przeznaczonym dla wideokonferencji nie może być pokój Komendantów lub Kierowników danej jednostki.