

Spis zawartości Programu Funkcjonalno-Użytkowego

I.	Wprowadzenie.....	3
II.	Zakres prac objętych przedmiotem zamówienia	5
III.	Szczegółowy opis prac	5
IV.	Szczegółowe wymagania techniczne głównych materiałów	8
V.	Założenia i wymagania Zamawiającego	11
VI.	Zakres dokumentacji.....	12
VII.	Ochrona własności.....	14
VIII.	Bezpieczeństwo i higiena pracy	14
IX.	Równoważność	14
X.	Termin realizacji.....	15
XI.	Warunki gwarancji i serwis	15
XII.	Przepisy prawne i normy związane z realizowanym zamierzeniem	16

I. Wprowadzenie

- 1) Podstawa prawna opracowania Ustawa z dnia 30.08.2024 Prawo zamówień publicznych (Dz.U. 2024 poz. 1320).
- 2) Przedmiot zamówienia należy wykonać w formule „zaprojektuj i wykonaj”.
- 3) W programie funkcjonalno-użytkowy określono podstawowe wymagania dla przedmiotu zamówienia umożliwiające sporządzenie dokumentacji projektowej budowlanej, technicznej i wykonawczej, na podstawie której zostaną wykonane roboty budowlane określone przez Zamawiającego w niniejszym opracowaniu.
- 4) Zamawiający oczekuje właściwej wiedzy i doświadczenia od Wykonawcy realizującego usługę budowy okablowania strukturalnego wraz z włączeniem urządzeń do istniejącej sieci.
- 5) Zamawiający oczekuje wykonania przedmiotu Zamówienia przez Wykonawcę gwarantującego zapewnienie dotychczasowego poziomu niezawodności i ciągłej dostępności systemów teleinformatycznych funkcjonujących w środowisku sieci.
- 6) Przed realizacją zadania Wykonawca przekaże do uzgodnienia dokumentację techniczną na podstawie, której zostanie wykonana realizacja. Dokumentacja ma być zgodna z zapisami znajdującymi się w punkcie „Zakres dokumentacji” oraz z **„Warunkami do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej”**. Dokumentację należy uzgodnić z:
 - Inspektorami branżowymi;
 - Działem Informatyki;
 - Administratorem budynku;
 - Administratorem wydziałowym;
 - Rzecznikiem ds. zabezpieczeń ppoż.
- 7) Wytyczne dotyczące realizacji przedmiotu zamówienia:
 - Wykonawca zapewni obecność Kierowników Robót posiadających uprawnienia do kierowania robotami budowlanymi bez ograniczeń w specjalności:
 - Telekomunikacyjnej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń telekomunikacyjnych);
 - Elektrycznej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych);
 - Sanitarnej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń cieplnych);
 - Wykonawca powinien dysponować osobami posiadającymi uprawnienia do projektowania bez ograniczeń w specjalności:
 - Telekomunikacyjnej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń telekomunikacyjnych);
 - Elektrycznej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń elektrycznych i elektroenergetycznych);
 - Sanitarnej (w specjalności instalacyjnej w zakresie sieci, instalacji i urządzeń cieplnych);

- Uzyskania pozwolenia Zamawiającego - Rektora lub Prorektora ds. wojskowych na wstęp na teren dla zatrudnionych cudzoziemców, zgodnie z procedurami obowiązującymi u Zamawiającego;
- Zamawiający informuje, że wskazany obiekt jest w ciągłym użytkowaniu, zakres prac będzie realizowany podczas bieżącego użytkowania obiektu;
- Roboty głośne np. wiercenia, kucia, wbijanie, stukanie, szlifowania mechaniczne można prowadzić tylko i wyłącznie po uzgodnieniu z użytkownikiem obiektu;
- Zamawiający informuje, że obiekt jest na gwarancji, dlatego dokumentację projektową i wszystkie prace należy uzgodnić z gwarantem obiektu.

II. Zakres prac objętych przedmiotem zamówienia

- Wykonanie i uzgodnienie projektu wykonawczego;
- Wykonanie prac przygotowawczych związanych między innymi z zabezpieczeniem/wyniesieniem, a na zakończenie prac wniesieniem urządzeń/mebli/instalacji wskazanych przez Użytkownika;
- Montaż kanałów elektroinstalacyjnych, kanałów podłatowych, gniazd natynkowych, desk boxów;
- Wykonanie instalacji sieci teleinformatycznej;
- Dostawa urządzeń aktywnych: przełączników sieciowych dostępowych i agregacyjnego wraz z niezbędnym oprogramowaniem i licencjami;
- Budowa tablicy rozdzielczej dla potrzeb zasilania gniazd DATA i szafek 12U;
- Podłączenie rozdzielni elektrycznej do rozdzielni znajdującej się w węźle budynkowym;
- Wykonanie instalacji elektrycznej zasilającej 2x230V DATA;
- Dostawa, uruchomienie UPS napięcia gwarantowanego (podtrzymanie min. 15 minut);
- Opis i oznaczenie kabli i urządzeń zgodnie z zasadami obowiązującymi w WAT;
- Dostawa i montaż klimatyzacji;
- Wykonanie pomiarów;
- Wywóz i utylizację odpadów oraz zdemontowanych elementów wyposażenia/urządzeń zgodnie z obowiązującymi przepisami w tym zakresie (Zamawiający zastrzega sobie prawo do zachowania wybranych demontowanych elementów wyposażenia pomieszczeń teleinformatycznych);
- Wykonanie i odtworzenie przejść pożarowych.

III. Szczegółowy opis prac

1) Sieć strukturalna i zasilająca DATA

- Dostawa i budowa trzech kabli światłowodowych MM 12G w relacji od istniejącej szafy teletechnicznej do szafek teletechnicznych 12U zamontowanych na poziomie parteru (dwie szafki) i piętra (jedna szafka);
- Rozszycie kabli światłowodowych (w istniejącej szafie panel światłowodowy należy zamontować w miejscu wskazanym przez Zamawiającego; kable światłowodowe należy rozszyc na jednym panelu);

- Wykonawca będzie prowadził wszystkie prace pod nadzorem Inspektorów WAT właściwych dla określonych branż;
- Wykonawca przygotowuje szczegółowe Specyfikacje Techniczne Wykonania i Odbioru Robót (STWiOR) zgodnie z zakresem ujętym w dokumentacji projektowej zatwierdzonej przez Zamawiającego;
- Wykonawca wykona kosztorysy ofertowe z podziałem na występujące branże wraz z zestawieniem kosztów zadania (ZKZ) całości przedmiotu zamówienia;
- Wykonawca przygotowuje szczegółowe kosztorysy ofertowe wykonania robót (zgodnie z aktualnymi cenami i podziałem na branże z ZKZ Oferty przetargowej) zgodne z zakresem robót ujętych w dokumentacji projektowej wykonawczej, technicznej po zatwierdzeniu rozwiązań projektowych przez Zamawiającego;
- Zamawiający wymaga sprawowania nadzoru autorskiego nad realizacją zadania (koszt nadzoru autorskiego po stronie Wykonawcy);
- Zakup, dostawa, montaż materiałów /urządzeń/ wyposażenia w zakresie Wykonawcy;
- Wykonawca wykonana prace przygotowawcze związane między innymi z:
 - Przygotowaniem wskazanych obszarów do prowadzenia prac montażowych;
 - Zabezpieczeniem miejsc w pobliżu prowadzenia prac montażowych;
 - Przygotowaniem miejsc na składowanie materiałów oraz odpadów powstałych w czasie wykonywania prac;
- Warunkiem rozpoczęcia prac jest uzyskanie zatwierdzenia przez Zamawiającego projektów wykonawczych oraz zatwierdzenie wniosków materiałowych;
- Zamawiający nie udostępni pomieszczeń lub możliwości wynajęcia na potrzeby socjalne, magazynowe;
- Zamawiający wymaga od Wykonawcy:
 - Bieżącego utrzymywania porządku na drogach komunikacyjnych oraz w obszarach, z których będzie korzystać w trakcie wykonywania prac;
 - Prawidłowego wykonania, odtworzenia wszystkich elementów budowlanych, które zostały zniszczone, rozebrane, uszkodzone w trakcie realizacji prac a nie były w zakresie zadania;
 - Zachowania w tajemnicy wszelkich informacji, uzyskanych w trakcie realizacji Umowy od dnia jej podpisania, przez czas nieoznaczony w szczególności nie umieszczanie nigdzie informacji o wykonywanych pracach bez zgody Zamawiającego. W przypadku naruszenia niniejszego obowiązku Zamawiający może dochodzić odszkodowania na zasadach ogólnych określonych w Kodeksie Cywilnym;
 - Wejścia na ten teren strefy obszaru chronionego wyłącznie na podstawie ważnej przepustki osobowej, natomiast wjazd/wyjazd pojazdów samochodowych (z wyłączeniem osobowych) Wykonawcy, zabezpieczających realizację przedmiotu umowy na terenie strefy obszaru chronionego – na podstawie ważnej przepustki osobowej kierowcy i przepustki na samochód;

- Wykonanie pomiarów okablowania światłowodowego (protokoły pomiarowe wraz ze świadectwem wzorcowania miernika dołączyć do dokumentacji powykonawczej);
- Doposażenie istniejącej szafy teletechnicznej w panel światłowodowy ze złączami światłowodowymi MM LC duplex, organizery kabli i przełącznik agregujący z wymaganą ilością wkładek SFP;
- Montaż, konfiguracja i uruchomienie przełącznika agregującego;
- Budowa sieci strukturalnej (kable typu F/FTP kat. 6A) w relacji od szafek teletechnicznych do modułów natynkowych (moduł natynkowy X xRJ45 + 2x 230V DATA, gdzie X – oznacza ilość gniazd RJ 45 i zależy od lokalizacji modułu);
- Budowa okablowania strukturalnego kat. 6A w relacji od gniazd natynkowych do desk boxów (Desk Box – 1x RJ45 + 2x 230V DATA; lokalizacja do ustalenia z Użytkownikiem);
- Wykonanie pomiarów okablowania strukturalnego (protokoły pomiarowe wraz ze świadectwem wzorcowania miernika dołączyć do dokumentacji powykonawczej);
- Dostawa, montaż listew kablowych, kanałów instalacyjnych, maskownic kablowych na potrzeby układania kabli sieci strukturalnej;
- Dostawa i montaż organizatorów na kable (montaż pod blatem biurka);
- Dostawa i montaż złączy (klamer) do połączenia biurek (min. 2 na jedno połączenie);
- Dostawa, montaż, konfiguracja i uruchomienie przełączników dostępowych;
- Dostawa kabli krosowych i patchcordów połączeniowych;
- Dostawa i montaż aktywnych światłowodowych kabli HDMI o długości min. 20m w relacji biurko wykładowcy – projektor we wskazanych lokalizacjach;
- Budowa instalacji zasilania 2x 230V DATA (lokalizacja gniazd zasilających przy gniazdach RJ45; należy przyjąć 6 gniazd pojedynczych 230V na jeden obwód uwzględniając gniazda w desk boxach);
- Budowa instalacji zasilania do desk boxów;
- Budowa instalacji zasilania do szafek teletechnicznych;
- Dostawa i montaż listew kablowych, kanałów instalacyjnych, maskownic kablowych na potrzeby układania kabli sieci zasilającej;
- Wykonanie pomiarów instalacji zasilania (protokoły pomiarowe wraz ze świadectwem wzorcowania miernika i uprawnieniami pomiarowców dołączyć do dokumentacji powykonawczej).

2) Budowa rozdzielni napięcia gwarantowanego

- Na potrzeby zasilania gwarantowanego urządzeń i odbiorów, w tym punktów dystrybucyjnych instalacji okablowania strukturalnego oraz gniazd DATA, należy przewidzieć zasilacz UPS. Na etapie projektu należy wykonać bilans mocy oraz dobrać zasilacz UPS.
- Budowa nowej rozdzielni elektrycznej (dostosowanej do standardu obowiązującego na obiekcie) na potrzeby zasilania stanowisk komputerowych (lokalizacja rozdzielni w pomieszczeniu rozdzielni elektrycznej obok rozdzielni istniejącej; na potrzeby zasilania należy wybudować tablice rozdzielcze z

- zabezpieczeniami przepięciowymi, zabezpieczeniami nadprądowymi, wyłącznikami różnicowo prądowymi typu „A” i lampkami sygnalizacyjnymi informującymi o uszkodzeniu zabezpieczenia);
- Budowa instalacji uziemiającej i wyrównawczej potencjałów wykonanej za pomocą przewodów typu „linka żo”, Lgy żo $\geq 16\text{mm}^2$ wraz z lokalną szyną wyrównawczą LSW oraz podłączeniem jej do istniejącej budynkowej instalacji wyrównawczej;
 - W rozdzielni należy:
 - Wykonać miedziane oszynowanie;
 - Wykonać wyprowadzenia wszystkich przewodów na złączki szynowe;
 - Zachować rezerwę miejsca i mocy min. 30%;
 - zastosować układ sieciowy TN-S z oddzielną szyną ochronną PE i neutralną N;
 - szafę zabezpieczyć zamkiem lub wkładką patentową;
 - Budowa bypassu zewnętrznego przełączenia zasilania UPS na sieciowe;
 - Dostawa, montaż i uruchomienie UPS (podtrzymanie min. 15’.).

3) Klimatyzacja

- W pomieszczeniu rozdzielni elektrycznej montaż instalacji i jednostek klimatyzacji naściennej (min. 2x 5 kW) przeznaczonych do pracy ciągłej, całorocznej wraz ze sterownikiem pracy grupowej zapewniającej rotację pracy urządzeń z funkcją autostartu po zaniku napięcia;
- Wykonanie instalacji chłodniczej;
- Wykonanie instalacji grawitacyjnego odprowadzenia skroplin zakończonej w węźle cieplnym. Przy stosowaniu pomp skroplin wykonać awaryjne wyłączenie klimatyzatora w przypadku sygnału awarii z pompki skroplin;
- Wszystkie instalacje (elektryczne, sanitarne) należy zabezpieczyć w szynach aluminiowych lub blaszanych;
- Agregaty należy zamontować obok agregatów istniejących na dachu budynku na konstrukcji, min. 40 cm nad dachem, z uwzględnieniem zabezpieczenia połączenia dachowej, gum amortyzujących / tłumików oraz wyłącznikiem napięcia;
- Klasa energetyczna chłodzenia: min. A+.

4) Szacunkowe ilości

- Szafka kablowa 12U 600x600 z panelem wentylacyjnym – 3 kpl.;
- Przełączniki dostępne wraz wkładkami SFP (zgodny ze standardem obowiązującym w WAT) – 7 kpl.;
- Przełącznik agregujący wraz wkładkami SFP (zgodny ze standardem obowiązującym w WAT) – 1 kpl.;
- Panel światłowodowy MM 36x LC duplex wyposażony – 1 kpl.;
- Panel światłowodowy MM 12x LC duplex wyposażony – 3 kpl.;
- Patchpanel 48x RJ45 kat. 6A wyposażony – 7 kpl.;

- Organizery kabli – 15 szt.;
- Kable krosowe FTP kat. 6A o długości 0,5m – 229 szt.;
- kable krosowe FTP kat. 6A o długości 1m – 229 szt.;
- Kable krosowe FTP kat. 6A o długości 5m – 20 szt.;
- Patchcordeny światłowodowe – 8 szt.;
- Listwy zasilające z filtrem przeciwzakłóceń 19" 1U 5x230V – 3 kpl.;
- Ilość zestawów gniazd natynkowych:
 - 5x RJ-45 + 2x 230V DATA – 3 kpl.;
 - 4x RJ-45 + 2x 230V DATA – 33 kpl.;
 - 3x RJ-45 + 2x 230V DATA – 34 kpl.;
- Desk boxy (1x RJ45 + 2x 230V DATA) – 229 kpl.;
- Długość kabla Eth F/FTP kat. 6A – ok. 6270 m;
- Długość kabla światłowodowego MM 12G – ok. 152 m;
- Długość kabli zasilających – ok. 4272 m;
- Długość kanałów elektroinstalacyjnych sieć strukturalna i zasilająca – ok. 800 m;
- Maskownice podłogowe – ok. 122 m;
- Rozdzielnia elektryczna napięcia gwarantowanego – 1 kpl.;
- UPS – 1 kpl.;
- Organizery na kable (montaż pod blatem biurka) – 229 kpl.;
- Złącza (klamry) do połączenia biurek – 352 kpl.;
- Aktywne światłowodowe kable HDMI o długości min. 20m – 13 szt.

5) Przepusty kablowe

- W istniejących przepustach, które zostały uszkodzone na potrzeby prowadzenia nowych kabli należy wykonać zabezpieczenia ppoż zgodnie z obowiązującymi przepisami;
- Nowo powstałe przepusty należy zabezpieczyć masą ognioochronną o klasie ognioodporności nie mniej niż klasa ognioodporności ściany, w której przepust został zrobiony;
- Każdy przepust oznakować podając typ i rodzaj zastosowanej masy, materiałów.

IV. Szczegółowe wymagania techniczne głównych materiałów

- 1) Przełączniki dostępne i agregujące – parametry urządzeń zgodne ze standardem obowiązującym w WAT i z parametrami podanymi w opracowaniu „Warunki do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej” wer. 3.00 z 04.06.2024 r.
- 2) Szafy teletechniczne

- szafa wisząca jednosekcyjna o wysokości min. 12U;
- standard instalacji 19";
- głębokość szafy 600 mm;
- drzwi przednie z szybą z hartowanego szkła;
- 1-punktowe zamki (drzwi, przód, panele boczne);
- wykończenie powierzchni: kształtowniki krępowane, trawione, fosforowane, malowane lakierem proszkowym;
- 180° kąt otwierania drzwi;
- wpusty kablowe na dole i górze;
- Wentylator montowany w dachu szafy.

3) Kabel FTP kat. 6A

- Konstrukcja: F/FTP;
- Klasa EA;
- Przekrój AW: 4x2x23AWG;
- Przepustowość binarna (max): 10Gb/s (do 100m);
- Pasma częstotliwości (max): 500MHz;
- Powłoka: tworzywo bezhalogenowe, nierozprzestrzeniające płomienia, o ograniczonym wydzielaniu dymów i gazów korozyjnych;
- Klasa CPR: B2ca;
- Materiał żyły: żyły miedziane;
- Ekran: ekran foliowy.

4) Kabel światłowodowy

- Kabel światłowodowy MM OM3/OM4 12G;
- Konstrukcja kabla: kabel jednotubowy;
- Budowa kabla: luźna tuba;
- Taśma absorbująca wilgoć;
- Wzmocnienie kabla: włókno szklane;
- Powłoka: LSOH;
- Klasa CPR: B2ca.

5) Panel światłowodowy

- Ilość adapterów: 12x LC/PC duplex, 36xLC/PC duplex
- Komplet materiałów montażowych;

- Wysuwana szuflada;
- Min. 4 przepusty kablowe.

6) Panel 48 x FTP kat. 6_A z modułami kat. 6_A

- Wielkość paneli 1U z zagęszczeniem portów do 48 (numeracja portów na panelu);
- Możliwość zabezpieczenia przed nieautoryzowanym wpięciem i wypięciem;
- Panel powinien:
 - zapewnić możliwość kodowania kolorem;
 - posiadać podpórkę na wprowadzane kable (tylny uchwyt do mocowania kabli);
 - posiadać zaczepty uziemiające;
 - posiadać złącza IDC;
- Terminacja żył w module za pomocą technologii IDC. Żyły kabla instalacyjnego muszą być w obrębie kontaktu IDC unieruchomione;
- Ekranowanie modułu zapewniające ochronę 360°.

7) Moduły RJ45

- Forma zabudowy Keystone;
- Ekranowanie modułu zapewniające ochronę 360°;
- Moduły powinny posiadać przesłonę przeciwkurzową;
- Akceptacja żyły typu: drut AWG 23-26;
- Sekwencja i metoda terminacji T568A / T568B bez użycia specjalnych narzędzi;
- Parametry elektryczne i transmisyjne zgodne z kat. 6A 10 GBE wg. ISO/IEC 11801 AMD2:2010-04, EN 50173-1:2011-09, EN 60603-7-51:2011-01, IEC 60603-7-51:2010-03;
- PoE zgodnie z IEEE 802.3af i PoE+ zgodnie z IEEE 802.3at, 4PPoE zgodnie z IEEE 802.3bt.

8) Kanał elektroinstalacyjny

- Materiał: bezhalogenowy;
- Podwójny zamek wieczka zwiększający sztywność listwy;
- Odporność uderzeniowa: IK06;
- Stopień ochrony IP40.

9) Pod blatowy organizator na kable

- Montaż: uchwyty zaciskowe do blatu biurka;
- Uchwyty na kable zapobiegające zsuwaniu i płątaniu kabli;
- Klipsy ułatwiające prowadzenie i segregację przewodów;
- Długość dostosowana do długości blatu biurka.

10) UPS

- Zasilacz UPS typu on-line o podwójnej konwersji VFI-SS-111;
- Budowa modułowa pozwalająca na uzyskanie redundancji zapewniającej wysoką konfigurowalność oraz niski czas serwisu i naprawy.;
- Czas podtrzymania min. 15 minut dla mocy znamionowej zasilacza;
- Należy zapewnić wyłączenie napięcia wyjściowego z projektowanego zasilacza UPS przez urządzenie uruchamiające przeciwpożarowego wyłącznika prądu budynku tj. styk EPO zasilacza połączyć ze stykiem NO istn. przycisku przeciwpożarowego wyłącznika prądu za pomocą przewodu HDGs 2x1,5mm² o wytrzymałości ogniowej 90 minut. Zasilacz ma posiadać styk EPO, który po jego zwarcu spowoduje wyłączenie urządzenia.

Uwaga: do wyłączenia zasilacza UPS wykorzystać oddzielny styk NO przycisku PWP, niezależny od styku wyłączającego zasilanie obiektu - podanie napięcia na styk EPO może skutkować uszkodzeniem zasilacza. W razie konieczności istniejący przycisk PWP wymienić na taki, który będzie posiadał oddzielny styk NO.

V. Założenia i wymagania Zamawiającego

- Urządzenia dostarczone w ramach zamówienia muszą być wolne od wad prawnych i fizycznych oraz nie mogą nosić żadnych śladów użytkowania. Wymaga się, aby sprzęt był fabrycznie nowy, pochodził z oficjalnego kanału sprzedaży producenta dedykowanego na rynek polski oraz był wyprodukowany seryjnie, z uwzględnieniem wszystkich opcji konfiguracyjnych przewidzianych dla oferowanego modelu. Niedopuszczalne są produkty prototypowe, urządzenia długo magazynowane lub pochodzące z programów wyprzedażowych producenta. Sprzęt nie może znajdować się na listach „end-of-sale” ani „end-of-support” producenta;
- Ze względów kompatybilności elektromagnetycznej EMC i redukcji możliwych zakłóceń zdecydowano się oprzeć okablowanie miedziane na kablu i komponentach ekranowanych;
- Zakłada się, iż środowisko pracy okablowania będzie środowiskiem łagodnym tj. określonym, jako M1l1C1E1 wg. skali MICE zgodnie z EN 50173-1;
- Oferowane urządzenia muszą posiadać oznakowanie CE (deklarację zgodności CE załączyć do dokumentacji powykonawczej);
- Wymaga się zabudowy HD zapewniającą wysokie upakowanie portów, minimum 48 portów RJ45 na 1U;
- Użyte materiały między innymi kable, kanały kablowe itp. powinny być bezhalogenowe, trudnopalne, nierozprzestrzeniające ognia i emitujące niewielkie ilości dymu;
- Wszystkie komponenty okablowania (panele, kable liniowe, kable przyłączeniowe, gniazda abonenckie, panele krosowe) muszą pochodzić z jednolitej oferty producenta systemu okablowania i spełniać wymagania do objęcia wykonanej instalacji bezpłatną, 25-letnią standardową gwarancją systemową,

która nie wymaga dodatkowych przeglądów, potwierdzoną certyfikatem gwarancyjnym producenta systemu;

- Okablowanie wewnętrzne międzyszafowe ma być oparte o nowoczesne rozwiązania przeznaczone do kablowania serwerowni i data center, składające się z fabrycznie terminowanych połączeń ze złączem RJ45 zapewniające modułową zabudowę typu Plug & Play. Połączenia preterminowane mają:
 - Ułatwić prace serwisowe i rekonfiguracyjne;
 - Ułatwić szybki montaż;
 - Zapewnić fabryczną jakość i skuteczność;
 - Zapewnić oszczędność miejsca w szafach.

VI. Zakres dokumentacji

1) Projekt wykonawczy (dokumentacja techniczna) powinien zawierać:

- Część opisową;
- Część rysunkową;
- Zestawienie materiałów;
- Karty katalogowe materiałów wraz z certyfikatami;
- Oświadczenia projektanta i sprawdzającego;
- Wykaz norm i przepisów.

Do projektu należy dołączyć:

- Specyfikacje techniczne wykonania i odbioru robót w podziale na wszystkie branże;
- Informacje dotycząca bezpieczeństwa i ochrony zdrowia dla przedmiotowego zadania.

Dopuszcza się podział projektu na części:

- Instalacje elektryczne;
- Instalacje teletechniczne.

Wszystkie części/tomy projektu powinny być wykonane z uwzględnieniem aktualnych przepisów prawa, rozporządzeń i norm. W zakresie budowy nowego okablowania teletechnicznego dokumentacja ma być zgodna z „Warunkami do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej” wer. 3.0 z 04.06.2024 r.

Część opisowa powinna zawierać opis:

- Szczegółowych rozwiązań projektowej instalacji wraz niezbędnymi wyliczeniami/symulacjami mającymi wpływ na poprawność jej działania oraz zgodnych z wytycznymi Zamawiającego przekazanych w PFU;
- Zasilania urządzeń wraz z odpowiednimi wyliczeniami;
- Konfiguracji poszczególnych urządzeń;
- Integracji z innymi systemami;
- Pomiarów, które należy wykonać w ramach realizowanych prac;
- Oznaczeń urządzeń i osprzętu;

- Przejść pożarowych wraz ze sposobem ich uszczelnienia;

Część rysunkowa – do dokumentacji należy dołączyć:

- Schematy blokowe instalacji;
- Szczegółowe schematy połączeń;
- Schematy rozszycia kabli;
- Rzuty z naniesionymi urządzeniami, trasami okablowania;
- Widoki szaf;
- Detale pokazujące montaż urządzeń;
- Inne rysunki wymagane przez Zamawiającego;

Zestawienie materiałów – powinno zawierać listę wszystkich materiałów, które są niezbędne do wykonania prac. W zestawieniu wraz z typem, rodzajem materiału należy podać nazwę producenta, ilość z jednostką miary.

Karty katalogowe – do projektu należy karty katalogowe wszystkich materiałów wskazanych w części Zestawienie materiałów wraz z niezbędnymi certyfikatami/atestami potwierdzającymi możliwość użycia.

Oświadczenie o kompletności projektu muszą podpisać projektant wraz ze sprawdzającym posiadający odpowiednie uprawnienia budowlane. Do projektu należy dołączyć kopię uprawnień wraz z potwierdzeniem przynależności do branżowej izby inżynierów.

W projekcie należy wpisać aktualne normy, przepisy prawa z uwzględnieniem których projekt został wykonany. Na etapie pozyskiwania uzgodnień dopuszcza się przesłanie wersji elektronicznej projektu.

Uzgodniony projekt oraz zatwierdzenie wniosków materiałowych przez Zamawiającego są podstawą do rozpoczęcia prac budowlano – montażowych.

Należy dostarczyć Zamawiającemu 3 komplety dokumentacji projektowej w wersji papierowej, 1 komplet w formie elektronicznej. Pliki należy przesłać w wersji edytowalnej (pliki w formacie DWG, DOC i XLS) oraz wersji nieedytowalnej (PDF). Dokumentację projektową należy wykonać w języku polskim.

2) Dokumentacja powykonawcza

- Wykonawca w ramach zamówienia wykona dokumentację powykonawczą
- Dokumentacja powykonawcza powinna zawierać:
 - Spis treści;
 - Oświadczenie kierownika robót;
 - Karty materiałowe wraz z załącznikami;
 - Instrukcję konserwacji i utrzymania;
 - Protokoły pomiarowe z certyfikatem miernika oraz uprawnieniami pomiarowca i osoby sprawdzającej (uprawnienia o ile są wymagane);
 - Protokoły odbiorów częściowych lub robót zanikających;
 - Protokoły potwierdzające przeprowadzenie testów integracji z istniejącą infrastrukturą sieciową;

- Protokoły odbiorów;
 - Gwarancję na urządzenia;
 - Zaznaczenie zmian w dokumentacji projektowej wraz z akceptacją projektanta;
 - Opis oznaczenia szaf, gniazd, kabli;
 - Opis i oznaczenie przebiegów przez ściany, stropy i przejścia pożarowych;
 - Potwierdzenie przeprowadzenia szkoleń.
- Nie dopuszcza się dostarczenia dokumentacji projektowej jako dokumentacji powykonawczej.

Należy dostarczyć Zamawiającemu 3 komplety dokumentacji w wersji papierowej, 1 komplet w formie elektronicznej. Pliki należy przesłać w wersji edytowalnej (pliki w formacie DWG, DOC i XLS) oraz wersji nieedytowalnej (PDF). Dokumentację należy wykonać w języku polskim.

Wykonawca przekaze Zamawiającemu dane konfiguracyjne urządzeń wraz z listą loginów i haseł.

VII. Ochrona własności

Wykonawca ponosi całkowitą odpowiedzialność za naruszenie praw i szkody wyrządzone Zamawiającemu a także osobom trzecim powstałe w wyniku wadliwie wykonywanych prac.

VIII. Bezpieczeństwo i higiena pracy

Podczas realizacji robót Wykonawca będzie przestrzegać przepisów dotyczących bezpieczeństwa i higieny pracy. Wykonawca ma obowiązek zadbać, aby personel nie wykonywał pracy w warunkach niebezpiecznych, szkodliwych dla zdrowia oraz nie spełniających odpowiednich wymagań sanitarnych. Wykonawca zapewni i będzie utrzymywał wszelkie urządzenia zabezpieczające, socjalne oraz sprzęt i odpowiednią odzież dla ochrony życia i zdrowia osób zatrudnionych na budowie oraz dla zapewnienia bezpieczeństwa publicznego.

IX. Równoważność

Zamawiający dopuszcza inne rozwiązania niż istniejące, o parametrach nie gorszych niż dla wyspecyfikowanych urządzeń (kryteriami równoważności). Wykonawca musi zapewnić pełne wdrożenie oferowanego rozwiązania wraz z wymaganymi licencjami, przeszkoleniem użytkowników i administratorów systemu oraz zapewnić pełną współpracę z używanym obecnie środowiskiem informatycznym oraz systemem monitoringu. Urządzenia, które nie będą spełniały opisanych kryteriów lub nie będą zgodne z aktualnymi „Warunkami do projektowania i budowy sieci strukturalnych dla potrzeb różnych systemów w Wojskowej Akademii Technicznej”, dostępnymi na stronie <https://www.wojsko-polskie.pl/wat/regulacje-it/> z przyczyn bezpieczeństwa mogą nie zostać zaakceptowane przez Zamawiającego i połączone do sieci kampusowej. W celu uniknięcia jakichkolwiek nieporozumień przed przystąpieniem do realizacji należy każdorazowo uzgadniać (na każdym etapie prac: koncepcja, projekt, wykonanie):

- Infrastrukturę teletechniczną z Sekcją Infrastruktury Teleinformatycznej Działu Informatyki;

- Urządzenia aktywne z Sekcją Infrastruktury Usługowej Działu Informatyki.

X. Termin realizacji

Termin realizacji prac: 60 dni liczone od dnia podpisania Umowy.

XI. Warunki gwarancji i serwis

- Wykonawca zapewni Zamawiającemu co najmniej 36 miesięcy gwarancji na wykonane prace będące przedmiotem zamówienia;
- Zamawiający oczekuje od Wykonawcy przedstawienia harmonogramu przeglądów wraz z dokładnym określeniem wykonywanych czynności;
- Całość rozwiązania ma być objęta jednolitą, spójną 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną miedzianą i światłowodową wraz z kablami krosowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu. Podstawą gwarancji ma być udzielone przez producenta okablowania zapewnienie właściwych parametrów przez 25 następnych lat. Program gwarancyjny ma zapewnić spełnienie wymagań parametrów elektrycznych i transmisyjnych, określonych w aktualnie obowiązujących normach ISO/IEC 11801 oraz EN 50173-1 dla całości zainstalowanego systemu niezależnie od obecnych i przyszłych aplikacji. Gwarancja obejmuje swoim zakresem całość systemu okablowania od głównego punktu dystrybucyjnego do gniazda użytkownika, zawiera, więc okablowanie szkieletowe i poziome;
- W celu uzyskania tego rodzaju gwarancji cały system musi być zainstalowany przez firmę instalacyjną legitymującą się dyplomami ukończenia kursu kwalifikacyjnego przez zatrudnionych pracowników w zakresie: instalacji, pomiarów, nadzoru, wykrywania i eliminacji uszkodzeń oraz projektowania okablowania strukturalnego, zgodnie z normami międzynarodowymi oraz procedurami instalacyjnymi producenta okablowania;
- Okres gwarancji ma być standardowo udzielany przez producenta okablowania, tzn. na warunkach oficjalnych, ogólnie znanych, dostępnych i opublikowanych. Tym samym oświadczenia o specjalnie wydłużonych okresach gwarancji wystawione przez producentów, dostawców, dystrybutorów, pośredników, wykonawców lub innych nie są uznawane za wiarygodne i równoważne względem niniejszych wymagań. Okres gwarancji liczony jest od dnia, w którym podpisano protokół końcowego odbioru prac i producent okablowania wystawił certyfikat gwarancji;
- Po wykonaniu instalacji firma wykonawcza powinna zgłosić wniosek o certyfikację systemu okablowania do producenta. Przykładowy wniosek powinien zawierać: listę zainstalowanych elementów systemu zakupionych w autoryzowanej sieci sprzedaży w Polsce, imienną listę pracowników wykonujących instalację, wyciąg z dokumentacji powykonawczej podpisanej przez pracownika pełniącego funkcję nadzorującą (np. Kierownik Projektu) oraz wyniki pomiarów dynamicznych łącza/kanалу transmisyjnego (Permanent Link/Channel) wszystkich torów transmisyjnych według norm ISO/IEC 11801 lub EN 50173;

- W celu zagwarantowania Użytkownikowi najwyższej jakości parametrów technicznych i użytkowych, cała instalacja powinna być nadzorowana w trakcie budowy przez inżynierów ze strony producenta oraz zweryfikowana niezależnie przed odbiorem technicznym.

XII. Przepisy prawne i normy związane z realizowanym zamierzeniem

- Ustawa z dnia 7 lipca 2022 r. - Prawo budowlane (Dz. U. z 2022 r. poz. 1557) z późn. zmianami;
- Ustawa z dnia 29 września 2021 r.- Prawo ochrony środowiska (Dz.U. z 2021 r. poz. 1973) z późn. zmianami;
- Ustawa z dnia 15 kwietnia 2021 r. o odpadach (Dz.U. 2021 poz. 779) z późn. zmianami;
- Ustawa z dnia 20 lipca 2022 r. o ochronie przeciwpożarowej budynków (Dz. U. z 2022 r. poz. 1620) z późn. zmianami;
- Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz.U. z 2021 r. poz. 2454) z późn. zmianami;
- Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 25 czerwca 2021 r. w sprawie szczegółowego zakresu i formy projektu budowlanego. (Dz. U. z 2021 r., poz. 1169) z późn. zmianami;
- Rozporządzenie Ministra Inwestycji i Rozwoju z dnia 29 kwietnia 2019 r. w sprawie przygotowania zawodowego do wykonywania samodzielnych funkcji technicznych w budownictwie. (Dz. U. z 2019 r., poz. 831) z późn. zmianami;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 15 czerwca 2021 r. w sprawie systemów oceny zgodności, wzoru deklaracji zgodności oraz sposobu znakowania wyrobów budowlanych dopuszczanych do obrotu i powszechnego stosowania w budownictwie. (Dz. U. z 2021 r. poz. 1213) z późn. zmianami;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 17 września 2021 r. w sprawie uzgadniania projektu zagospodarowania działki lub terenu, projektu architektoniczno-budowlanego, projektu technicznego oraz projektu urządzenia przeciwpożarowego pod względem zgodności z wymaganiami ochrony przeciwpożarowej (Dz. U. z 2021 r., poz. 1722) z późn. zmianami;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 sierpnia 1998 r. w sprawie aprobat i kryteriów technicznych oraz jednostkowego stosowania wyrobów budowlanych. (Dz.U. 1998 nr 107 poz. 679 ze zm.) z późn. zmianami;
- Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 21 grudnia 2020 r. zmieniające rozporządzenie w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie. (Dz. U. z 2020 r. poz. 2351) z późn. zmianami;
- Rozporządzenie Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie. (Dz. U. z 2023 r. poz. 1040) z późn. zmianami;

- Obwieszczenie Ministra Inwestycji i Rozwoju z dnia 25 kwietnia 2018 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Infrastruktury w sprawie dziennika budowy, montażu i rozbiórki, tablicy informacyjnej oraz ogłoszenia zawierającego dane dotyczące bezpieczeństwa pracy i ochrony zdrowia. (Dz. U. z 2018, poz. 963) z późn. zmianami;
- Rozporządzenie Ministra Rozwoju z dnia 2 czerwca 2016 r. w sprawie wymagań dla sprzętu elektrycznego. (Dz. U. z 2016, poz. 806) z późn. zmianami;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych. (Dz. U. z 2009 r. Nr 124, poz. 1030) z późn. zmianami;
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz. U. z 2010 r. Nr 109, poz. 719) z późn. zmianami;
- Rozporządzenie Rady Ministrów z dnia 7 grudnia 2012 r. w sprawie rodzajów urządzeń technicznych podlegających dozorowi technicznemu (Dz. U. z 2012 r., poz. 1468) z późn. zmianami;
- Rozporządzenie Ministra Gospodarki z dnia 15 marca 2001 r. w sprawie wzoru znaku dozoru technicznego (Dz. U. z 2001 r., Nr 30, poz. 346) z późn. zmianami;
- Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r. w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz. U. z 2003 r., Nr 47, poz. 401) z późn. zmianami;
- Rozporządzenie Ministra Infrastruktury z dnia 23 czerwca 2003 r. w sprawie informacji dotyczącej bezpieczeństwa i ochrony zdrowia oraz planu bezpieczeństwa i ochrony zdrowia (Dz. U. z 2003 r. Nr 120, poz. 1126) z późn. zmianami;
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 31 marca 2021 r. w sprawie ogłoszenia jednolitego tekstu ustawy o planowaniu i zagospodarowaniu przestrzennym. (Dz. U. z 2021 r., poz. 741) z późn. zmianami;
- Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 czerwca 2021 r. w sprawie ogłoszenia jednolitego tekstu ustawy o wyrobach budowlanych (Dz. U. z 2021 r., poz. 1213) z późn. zmianami;

Normy i ich aktualizacje:

- PN-EN 50173-1 System okablowania strukturalnego z przeznaczeniem do budynków biurowych;
- EN 60603-7-51 Szczegółowe wymagania dla 8 – polowych, ekranowanych, wolnych i stałych złączy do transmisji danych o częstotliwości do 500 MHz;
- PN-78/B-10440 Wentylacja mechaniczna - Urządzenia wentylacyjne - Wymagania i badania przy odbiorze;
- Temperatury ogrzewanych pomieszczeń w budynkach. PPN-71/B-02380 - Oświetlenie wnętrz światłem dziennym – wymagania PN-ISO 6242 - 1: 1999 - Budownictwo - Wyrażanie wymagań użytkownika - Wymagania termiczne;

- PN-ISO 6242 - 2: 1999 Budownictwo - Wyrażanie wymagań użytkownika - Wymagania dotyczące czystości powietrza dotyczących oceny własności użytkowych;
- PN-ISO - 8756: 2000 Jakość powietrza - postępowanie z danymi dotyczącymi temperatury, ciśnienia i wilgotności;
- PN-EN 13300 Farby i lakiery – Klasyfikacja określająca jakość farb do wnętrz;
- PN-92/B-01706/Az1:1999 - Instalacje wodociągowe - Wymagania w projektowaniu (zmiana Az1);
- PN-N - 18002: 2000 - Systemy zarządzania bezpieczeństwem i higieną pracy - Ogólne wytyczne do oceny ryzyka zawodowego;
- Aktualne normy elektryczne;
- Zarządzenie Nr 28/RKR/2024 z dnia 05.06.2024 r „Warunki do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej” wersja 3.00 z dnia 04 czerwca 2024 r.;
- Wymagania eksploatacyjno-techniczne dla XIX grupy SpW – systemy i urządzenia specjalistyczne do ochrony obiektów” z dnia 08 maja 2020 r;
- EN 50174-2:2018-08 Technika informatyczna -- Instalacja okablowania -- Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków;
- EN 50174-1:2018-08 Technika informatyczna -- Instalacja okablowania - Część 1: Specyfikacja instalacji i zapewnienie jakości;
- EN 50346:2004/A2:2010 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania;
- ISO/IEC 11801-1:2017 Information technology - Generic cabling for customer premises - Part 1: General requirements;
- ISO/IEC 27001:2023-08 Technika informatyczna -- Techniki bezpieczeństwa -- Systemy zarządzania bezpieczeństwem informacji -- Wymagania;
- ISO/IEC 20000-1:2014-01 Technika informatyczna -- Zarządzanie usługami -- Część 1: Wymagania dla systemu zarządzania usługami.

Załączniki:

„Warunki do projektowania i budowy sieci strukturalnych dla potrzeb różnych systemów w Wojskowej Akademii Technicznej”

WOJSKOWA AKADEMIA TECHNICZNA

im. Jarosława Dąbrowskiego

**„ZATWIERDZAM”
REKTOR-KOMENDANT
WOJSKOWEJ AKADEMII TECHNICZNEJ
im. Jarosława Dąbrowskiego**

gen. bryg. prof. dr hab. inż. Przemysław WACHULAK
/podpisano kwalifikowanym podpisem cyfrowym/



WARUNKI DO PROJEKTOWANIA I BUDOWY SIECI STRUKTURALNYCH DLA POTRZEB SYSTEMÓW W WOJSKOWEJ AKADEMII TECHNICZNEJ

Wersja dokumentu: 3.00
Data wersji: 04.06.2024 r.

**DZIAŁ INFORMATYKI
WARSZAWA 2024**

Spis treści

1	CEL I ZAKRES DOKUMENTU	4
2	DEFINICJE POJĘĆ PODSTAWOWYCH	4
3	CHARAKTERYSTYKA SYSTEMU OKABLOWANIA STRUKTURALNEGO.....	5
4	WYMAGANIA W ZAKRESIE DOBORU KOMPONENTÓW OKABLOWANIA STRUKTURALNEGO	6
4.1	Założenia podstawowe.....	6
4.2	Założenia szczegółowe	7
4.2.1	Opis wymagań pod okablowania pionowe	7
4.2.2	Wymagania dotyczące podsystemu okablowania poziomego abonenckiego	12
4.3	Administracja, etykietowanie	15
4.4	Wymagania gwarancyjne	15
4.5	Odbiory.....	16
5	WYMAGANIA DOTYCZĄCE KANALIZACJI TELETECHNICZNEJ I PROWADZENIA KABLI ZEWNĘTRZNYCH	16
5.1	Telekomunikacyjne kable miedziane	17
5.2	Przywieszki identyfikacyjne.....	17
5.3	Wprowadzenia kanalizacji kablowej do budynków.....	18
6	WYMAGANIA W ZAKRESIE SERWEROWNI BUDYNKOWYCH / GPD / PPD	19
7	WYMAGANIA W ZAKRESIE ZASILANIA SIECI TELEINFORMATYCZNYCH	19
8	WYMAGANIA W ZAKRESIE URZĄDZEŃ AKTYWNYCH	20
8.1	Wymagania ogólne dla urządzeń i oprogramowania sieciowego	20
8.2	Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania sieciowego	20
8.3	Urządzenia do sieci resortowych	21
8.4	Urządzenia do Kampusowej Sieci Bezprzewodowej (KSB).....	21
8.4.1	Wymaganie ogólne.....	21
8.4.2	Przyjęty standard.....	21
8.4.3	Dopuszczone urządzenia i akcesoria sieciowe do KSB	22
8.4.4	Wymagania dla firmy odpowiadającej za montaż i konfigurację	22
8.5	Urządzenia do Akademickiej Sieci Komputerowej.....	23
8.5.1	Przyjęty standard.....	23
8.5.2	Równoważność	23
8.5.3	Routery	23
8.5.4	Przełączniki dostępowe Typ 1	27
8.5.5	Przełączniki dostępowe Typ 2	31
8.5.6	Przełączniki agregujące Typ 1.....	35
8.5.7	Przełączniki agregujące Typ 2.....	39
8.6	Urządzenia do obsługi ruchu CCTV	43
9	WYMAGANIA W ZAKRESIE OKABLOWANIA SYSTEMÓW OCHRONY TECHNICZNEJ	43
9.1	Przewody miedziane	44
9.2	Przewody światłowodowe	45
9.3	Zasilanie systemu	45
10	WYMAGANIA W ZAKRESIE SYSTEMÓW SSP	46
11	WYMAGANIA W ZAKRESIE INTEGRACJI SYSTEMÓW OCHRONY TECHNICZNEJ WAT	46
12	DOBÓR LICZBY WŁÓKIEN ŚWIATŁOWODOWYCH.....	46

13	NORMY REFERENCYJNE	47
14	SPIS RYSUNKÓW I TABEL	49
15	HISTORIA WERSJI	50

1 CEL I ZAKRES DOKUMENTU

Celem dokumentu jest przedstawienie warunków do:

- 1) usprawnienia procesu opracowywania i uzgadniania dokumentacji projektowych;
- 2) budowy w Wojskowej Akademii Technicznej (WAT) stosunkowo jednolitej (pod względem technicznym) infrastruktury teleinformatycznej;
- 3) budowy okablowania strukturalnego umożliwiającego implementację rozwiązań spełniających wymagania techniczne i bezpieczeństwa.

2 DEFINICJE POJĘĆ PODSTAWOWYCH

- 1) **Akademicka Sieć Komputerowa (ASK)** – zespół środków technicznych i organizacyjnych służących do realizacji połączeń i transmisji danych pomiędzy jednostkami organizacyjnymi WAT oraz do wymiany informacji z innymi sieciami, w szczególności z siecią Internet;
- 2) **główny punkt dystrybucyjny (GPD)** – punkt dystrybucyjny, w którym kończy(-a) się budynkowy(-e) kabel(-le) szkieletowy(-e), i w którym są wykonane połączenia z węzłem szkieletowym ASK (kablami szkieletowymi);
- 3) **kabel szkieletowy** – kabel łączący węzeł dystrybucyjny ASK z głównym punktem dystrybucyjnym w budynku;
- 4) **kabel pionowy** – kabel łączący główny punkt dystrybucyjny w budynku z piętrowym punktem dystrybucyjnym, budynkowe kable szkieletowe mogą także łączyć piętrowe punkty dystrybucyjne w tym samym budynku;
- 5) **kabel poziomy** – kabel łączący piętrowy/budynkowy punkt dystrybucyjny z gniazdem telekomunikacyjnym;
- 6) **kabel połączeniowy** – kabel służący do podłączenia urządzenia końcowego do gniazda telekomunikacyjnego;
- 7) **kabel krosowy** – kabel stosowany do ustanawiania połączeń w panelu krosowym;
- 8) **węzeł dystrybucyjny ASK** – punkt dystrybucyjny, który skupia okablowanie szkieletowe;
- 9) **punkt dystrybucyjny (PD)** – miejsce koncentracji, zbioru komponentów (na przykład paneli krosowych, kabli krosowych) stosowanych do łączenia kabli;
- 10) **panel krosowy** – panel służący do zestawienia połączeń pomiędzy elementami (urządzeniami) współpracującymi w ramach systemu okablowania strukturalnego;
- 11) **gniazdo telekomunikacyjne** – miejsce zakończenia kabla poziomego;
- 12) **punkt elektryczno-logiczny abonencki (PEL)** – (PEL = gniazda telekomunikacyjne + gniazda elektryczne) miejsce zakończenia kabla poziomego oraz kabla zasilania wydzielonego dla sieci teleinformatycznej;
- 13) **okablowanie strukturalne** – system telekomunikacyjnych kabli połączeniowych i krosowych oraz osprzętu połączeniowego umożliwiający działanie sprzętu i urządzeń teleinformatycznych.

3 CHARAKTERYSTYKA SYSTEMU OKABLOWANIA STRUKTURALNEGO

Istotą zastosowania okablowania strukturalnego jest możliwość współdzielenia zasobów w ramach jednej instalacji przez wiele systemów teleinformatycznych i teletechnicznych.

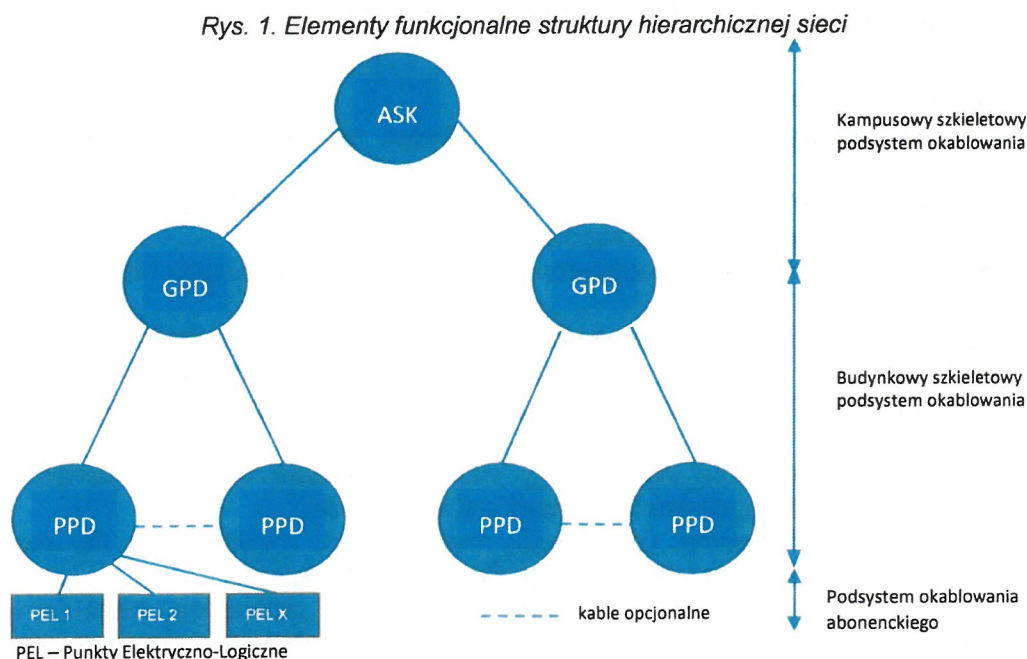
Na system okablowania strukturalnego składają się podsystemy okablowania:

- 1) szkieletowego kampusowego;
- 2) szkieletowego budynkowego;
- 3) poziomego abonenckiego.

Okablowanie systemu strukturalnego budowane jest w oparciu o połączenia fizyczne z wykorzystaniem topologii gwiazdy rozszerzonej. W skład podsystemów okablowania strukturalnego wchodzi następujące elementy funkcjonalne:

- 1) węzeł dystrybucyjny ASK;
- 2) kampusowe kable szkieletowe;
- 3) GPD;
- 4) budynkowy kabel szkieletowy (okablowanie pionowe);
- 5) piętrowy punkt dystrybucyjny (PPD);
- 6) kable telekomunikacyjne pomiędzy punktami dystrybucyjnymi a abonenckimi punktami elektryczno-logicznymi (okablowanie poziome);
- 7) kabel połączeniowy (PEL – urządzenie końcowe).

Poszczególne elementy funkcjonalne są łączone ze sobą w celu uzyskania struktury hierarchicznej przedstawionej na Rys. 1.



Zgodnie z normami w zależności od rozległości okablowania strukturalnego, można wyróżnić następujące jego podsystemy:

- 1) Kampusowy szkieletowy podsystem okablowania, obejmujący:
 - a) węzeł ASK połączony z głównym budynkowym punktem dystrybucyjnym,
 - b) kampusowe kable szkieletowe,

- c) mechaniczne zakończenia kampusowych kabli szkieletowych w węźle ASK i GPD wraz z kablami krosowymi,
- d) kable łączące w węźle ASK;
- 2) Budynkowy szkieletowy podsystem okablowania strukturalnego, obejmujący:
 - a) GPD budynku połączony z PPD,
 - b) budynkowe kable szkieletowe (okablowanie pionowe),
 - c) mechaniczne zakończenia budynkowych kabli szkieletowych w GPD i PPD wraz z kablami krosowymi w GPD,
 - d) połączenia wewnątrzbudynkowe pomiędzy poszczególnymi PPD – wyłącznie jako okablowanie dodatkowe i nadmiarowe w stosunku do okablowania wymaganego przez podstawową topologię hierarchiczną;
- 3) Podsystem okablowania poziomego abonenckiego, obejmujący:
 - a) PPD,
 - b) kable miedziane typu skrętka nieekranowana lub ekranowana kategorii 6A,
 - c) PEL.

Nie zakłada się obowiązku obligatoryjnego stosowania w każdej inwestycji wszystkich wymienionych podsystemów okablowania (komponentów). Wyboru, czy i jakie elementy występują w podsystemie okablowania, dokonuje się na etapie projektowym, biorąc pod uwagę: specyfikę obiektu, rozległość instalacji oraz względy funkcjonalno-użytkowe.

4 WYMAGANIA W ZAKRESIE DOBORU KOMPONENTÓW OKABLOWANIA STRUKTURALNEGO

4.1 Założenia podstawowe

Do projektów budowy okablowania strukturalnego należy przyjąć następujące założenia:

- 1) wszystkie produkty wchodzące w skład systemu okablowania strukturalnego muszą pochodzić z oferty jednego producenta;
- 2) użyte elementy z oferty producenta winny być oznaczone logo tego samego producenta;
- 3) producent okablowania strukturalnego musi udzielić minimum 25-letniej gwarancji na oferowany system, zabezpieczając Użytkownika przed nieprawidłowym działaniem poszczególnych komponentów i przed problemami instalacyjnymi;
- 4) produkty tworzące tor transmisyjny muszą posiadać właściwe certyfikaty stwierdzające ich zgodność z normami referencyjnymi;
- 5) podsystem okablowania poziomego musi zostać zrealizowany na bazie systemu ekranowanego o wydajności klasy EA/ kat. 6A;
- 6) w części światłowodowej podsystem okablowania pionowego musi zostać oparty na okablowaniu wielomodowym i jednomodowym (zwanym dalej odpowiednio: MM oraz SM). Okablowanie MM ma charakteryzować się wydajnością OF-300, natomiast SM wydajnością OF-2000 oraz kategorią włókien odpowiednio OM3 lub OM4 i OS2 według **ISO/IEC 11801 Ed.2.2: 2011**. Interfejsem światłowodowym stosowanym w kampusowym szkielecie sieci jest LC/APC duplex, a w pozostałej części sieci LC/PC duplex;
- 7) w części miedzianej (kable telekomunikacyjne):

- a) podsystem okablowania pionowego budynkowego do połączenia PPD z GPD ma zostać oparty na telekomunikacyjnym (T) kablu (K) miejscowym (M), pęczkowym – czwórkowym, o izolacji z polietylenu piankowego z cienką warstwą polietylenu jednolitego (Xp), o powłoce polietylenowej z zaporą przeciwwilgociową (Xz), wypełniony żelazem (w) – **XzTKMXpw, 10-200x4x0,5** (od 10 do 200 „czwórek” w zależności od potrzeb), obustronnie rozsztytym na panelach ISDN kat. 3,
- b) podsystem budynkowego okablowania szkieletowego ma zostać oparty na kablu wieloparowym 30/50/100-parowym, kategorii 3;
- 8) GPD i PPD należy projektować w szafach dystrybucyjnych 19” RACK o wymiarach dostosowanych do potrzeb. W przypadku zastosowania szaf wolnostojących, zaleca się zastosowanie szaf o wymiarach 800x1000x2200 mm;
- 9) zastosowany system okablowania strukturalnego musi charakteryzować się najwyższą elastycznością niezbędną do ewentualnych rozbudów sieci w czasie użytkowania oraz walorami użytkowymi pozwalającymi na bezproblemową i bezpieczną obsługę systemu przez użytkownika;
- 10) okablowanie stosowane do projektowania i budowy sieci strukturalnych dla potrzeb systemów w Wojskowej Akademii Technicznej powinno spełniać wymagania rozporządzeniem Parlamentu Europejskiego i Rady Europejskiej nr 305/2011 z dnia 9 marca 2011 r.

4.2 Założenia szczegółowe

Projektowany system okablowania strukturalnego dla budynku powinien spełniać wymagania określone w rozdziale 3.

4.2.1 Opis wymagań pod okablowania pionowe

4.2.1.1 Połączenia szkieletowe światłowodowe

Światłowodowe połączenia szkieletowe przeznaczone są do obsługi protokołów transmisji danych. Realizacja tych połączeń powinna następować poprzez standardowe połączenia oparte na kablu instalacyjnym, spawanie włókien kabli preterminowanych fabrycznie odpowiednim złączem.

4.2.1.2 Instalacyjny kabel światłowodowy

W celu umożliwienia realizacji światłowodowych połączeń szkieletowych pionowy podsystem okablowania strukturalnego powinien zostać oparty na kablu spełniającym wymagania, które określa *Tabela 1*.

Tabela 1. Wymagane parametry kabla światłowodowego

Kat. kabla wg ISO11801 ed.2.2	OM3/OM4	OS2
Konstrukcja kabla wg DIN VDE 0888	A/I-DQ(ZN)BH	A/I-DQ(ZN)BH
Konstrukcja kabla wg ZN-TF-11:2001; ZN-EK-103 dla kanalizacji ziemnych	Z-XOTKtsd	Z-XOTKtsd
Powłoka zewnętrzna	Uniwersalna	Uniwersalna
Budowa kabla	Luźna tuba	Luźna tuba
Taśma absorbująca wilgoć	tak	tak
Ochrona przeciw gryzoniom	tak	tak
Wzmocnienie kabla A/I-DQ(ZN)BH / Z-XOTKtsd	Włókno szklane /Dielektryczny pręt FRP w powłoce z polietylenu lub bez powłoki	Włókno szklane /Dielektryczny pręt FRP w powłoce z polietylenu lub bez powłoki
Klasyfikacja ogniowa powłoki zew.	LSZH	LSZH

Standardy klasyfikacji ogniowej (uwzględniające wytyczne CPR)	IEC 60332-1 test na rozchodzenie się ognia; IEC 60754-2 test na stopień kwasowości gazów; IEC 61034 test na gęstość zadymienia.
--	---

4.2.1.3 Kable światłowodowe preterminowane

Połączenia oparte na złączach MPO

Połączenia szkieletowe preterminowane należy realizować za pomocą kabli zakończonych fabrycznie na obu końcach złączem MPO zgodnym z IEC 61754-7. Kable o takiej konstrukcji mają być zainstalowane bezpośrednio w panelach krosowych opisanych w dalszej części niniejszych zaleceń. Podstawowe parametry zalecanych kabli przedstawia *Tabela 2*.

Tabela 2. Wymagane parametry kabla światłowodowego preterminowanego złączami typu MPO

Rodzaj włókien	jednomodowe	wielomodowe
Kategoria włókien	OS2	OM3/OM4
Liczba włókien	12/24	12/24
Szlif złącza	PC	PC
Polaryzacja zgodnie z TIA-568-C	A/B	A/B
Średnie straty wtrąceniowe (IL) zgodnie z IEC 61300-3-34	≤0,2 dB	≤0,5 dB
Straty wtrąceniowe (RL) zgodnie z IEC 61300-3-6	≥35 dB	≥26 dB
Ilość cykli połączeniowych	<1000	<1000
Kolorystyka powłoki zgodnie z ISO 11801 ed.2.2.	żółta	turkusowa
Max zewnętrzna średnica kabla	3 mm (12 wł.), 6 mm (24 wł.), 9 mm (48 wł.), 11,2 (72 wł.)	
Klasyfikacja ogniowa powłoki zew.	LSZH	LSZH
Standardy klasyfikacji ogniowej dla powłok (uwzględniające wytyczne CPR)	IEC 60332-1 test na rozchodzenie się ognia IEC 60754-2 test na stopień kwasowości gazów IEC 61034 test na gęstość zadymienia	

Połączenia oparte na złączach LC

Połączenia szkieletowe preterminowane należy realizować za pomocą kabli zakończonych fabrycznie na obu końcach złączami typu LC zgodnymi z IEC 61754-20. Kable o takiej konstrukcji powinny być zainstalowane bezpośrednio w panelach krosowych. Podstawowe parametry zalecanych kabli przedstawia *Tabela 3*.

Tabela 3. Wymagane parametry kabla światłowodowego preterminowanego złączami typu LC

Rodzaj włókien	jednomodowe	wielomodowe
Kategoria włókien	OS2	OM3/OM4
Liczba włókien	12/24/48/72/144	12/24/48
Szlif złącza	PC	PC
Średnie straty wtrąceniowe (IL) zgodnie z IEC 61300-3-34	≤0,25 dB	≤0,15 dB
Straty wtrąceniowe (RL) zgodnie z IEC 61300-3-6	≥55 dB	≥35 dB
Liczba cykli połączeniowych	<1000	<1000
Kolorystyka powłoki zgodnie ISO 11801 ed.2.2.	żółta	turkusowa
Max zewnętrzna średnica kabla	3 mm (12 wł.), 6 mm (24 wł.), 9 mm (48 wł.)	
Klasyfikacja ogniowa powłoki zew.	LSZH	LSZH

Standardy klasyfikacji ogniowej dla powłok
(uwzględniające wytyczne CPR)

IEC 60332-1 test na rozchodzenie się ognia
IEC 60754-2 test na stopień kwasowości gazów
IEC 61034 test na gęstość zadymienia

4.2.1.4 Światłowodowe panele krosowe

Wyspecyfikowane w p. 4.2.1.2 kable światłowodowe należy wprowadzić i zaterminować w panelach światłowodowych. Panele te muszą charakteryzować się szeregiem własności funkcjonalno-użytkowych pozwalających na sprawne, wygodne i oszczędne użytkowanie systemu okablowania przez cały okres jego eksploatacji.

Rozwiązania pod spawy światłowodowe i preterminowane

Panel typu panel HD:

- 1) Panel nie może zajmować więcej miejsca w szafie niż 1U;
- 2) Zagęszczenie portów musi zapewniać obsługę do 48 portów (max. 96 włókien światłowodowych);
- 3) Konstrukcja panelu musi charakteryzować się elastycznością pozwalającą na przyszłe rozbudowy/migracje sieci, tj. panel musi mieć możliwość obsługiwanie jednocześnie:
 - a) łączy optycznych minimum LC/PC, LC/APC w wersji spawanej i preterminowanej,
 - b) łączy miedzianych kategorii 6A,
 - c) dowolnej mieszanki wyżej wymienionych łączy;
- 4) Konstrukcja panelu musi gwarantować możliwość jego obsługi od przodu, co wydatnie usprawnia jego obsługę w przypadku ograniczonego dostępu do szafy z innych stron;
- 5) Panel musi umożliwiać zaimplementowanie systemu inteligentnego monitorowania portów w dowolnym momencie jego użytkowania bez konieczności rozłączania istniejących połączeń;
- 6) Panel musi posiadać wymienne pola opisowe pozwalające na etykietowanie połączeń. Dodatkowo każdy port musi być trwale ponumerowany;
- 7) Obudowa panelu powinna być w kolorze czarnym/szarym.

Kaseta światłowodowa (w powiązaniu z panelem HD):

- 1) Panel musi mieć możliwość instalacji kaset światłowodowych;
- 2) Kaseta światłowodowa musi stanowić element systemu bezpiecznego prowadzenia kabla instalacyjnego od miejsca jego wprowadzenia do szafy aż do wejścia do panelu;
- 3) Kasety muszą gwarantować minimum R35 promienia gięcia włókien wewnątrz kasety, co jest warunkiem koniecznym do uzyskania niskiej tłumienności włókna;
- 4) Kaseta musi umożliwiać terminację włókien na następujących złączach optycznych:
 - a) LC/PC duplex,
 - b) LC/APC duplex;
- 5) Kasety światłowodowe muszą umożliwiać wymianę panelu czołowego, co pozwoli na zmianę użytego standardu złączy w każdym momencie użytkowania;
- 6) Kasety światłowodowe muszą charakteryzować się konstrukcją pozwalającą na uzyskanie maksymalnej elastyczności rozumianej jako:
 - a) obsługa zarówno łączy preterminowanych, jak i spawanych,
 - b) tacka spawów musi mieć możliwość wykonania rezerwy ok. 1,5 m włókien z kabla instalacyjnego oraz minimum 2 m pigtaili w ramach kasety,

- c) możliwość wprowadzania kabla zarówno pod kątem 90°, jak i 45°,
- d) możliwość wykonania ok. 2 m rezerwy luźnej tuby w ramach kasety;
- 7) Kasety muszą stanowić kompletne rozwiązanie gotowe do wykonania spawów i zawierające:
 - a) komplet pigtaili,
 - b) komplet adapterów połączeniowych,
 - c) tackę spawów,
 - d) magazynki spawów,
 - e) komplet osłonek termokurczliwych lub alternatywnych,
 - f) system bezpiecznego wprowadzenia kabla do kasety.

Kasety i uchwyty do paneli HD

Kaseta światłowodowa breakoutowa:

- 1) Kaseta światłowodowa musi stanowić element systemu bezpiecznego prowadzenia kabla instalacyjnego od miejsca jego wprowadzenia do szafy aż do wejścia do panelu;
- 2) Kasety muszą gwarantować minimum R35 promienia gięcia kabli wewnątrz kasety, co jest warunkiem koniecznym do uzyskania niskiej tłumienności włókna;
- 3) Kaseta musi umożliwiać obsługę następujących złączy optycznych: LC/PC duplex;
- 4) Kasety światłowodowe muszą umożliwiać wymianę panelu czołowego, co pozwoli na zmianę użytego standardu złączy w każdym momencie użytkowania;
- 5) Kasety światłowodowe muszą charakteryzować się konstrukcją pozwalającą uzyskać maksymalną elastyczność rozumianą jako:
 - a) obsługa zarówno łączy preterminowanych, jak i spawanych,
 - b) możliwość wprowadzania kabla zarówno pod kątem 90°, jak i 45°,
 - c) możliwość wykonania ok. 1 m rezerwy wprowadzonego kabla;
- 6) Kasety muszą być wyposażone w komplet adapterów połączeniowych.

Kaseta światłowodowa MPO:

- 1) Kasety muszą gwarantować minimum R35 promienia gięcia kabli wewnątrz kasety, co jest warunkiem koniecznym do uzyskania niskiej tłumienności włókna;
- 2) Kaseta musi umożliwiać obsługę złączy optycznych LC duplex;
- 3) Kaseta musi charakteryzować się następującymi cechami:

Tabela 4. Wymagane parametry kasety światłowodowej typu MPO

Rodzaj obsługiwanych włókien	jednomodowe	wielomodowe
Kategoria włókien	OS2	OM4
Liczba włókien	12/24	12/24
Rodzaj złącza (strona A)	MPO	MPO
Szlif złącza (strona A)	PC	PC
Polaryzacja zgodnie z TIA-568-C	A/B	A/B
Rodzaj złącza (strona B)	LC duplex	LC duplex
Szlif złącza (strona B)	APC	PC
Średnie straty wtrąceniowe (IL per kaseta) zgodnie z IEC 61300-3-34	≤0,35 dB	≤0,30 dB
Straty wtrąceniowe (RL per kaseta) zgodnie z IEC 61300-3-6	≥50 dB	≥27 dB

Adaptory i złącza – wymagania w powiązaniu z panelami dla wersji spawanej i preterminowanej

Adaptory światłowodowe

Adaptory światłowodowe będące na wyposażeniu kaset powinny charakteryzować się następującymi własnościami:

- 1) zastosowane w adapterach połączeniowych tuleje powinny być ceramiczne, co poprawia mechaniczne własności adaptera (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia;
- 2) ze względów bezpieczeństwa adaptory oraz złącza stosowane w panelu muszą automatycznie zamykać prześwit włókna w feruli, tak aby zminimalizować niebezpieczeństwo uszkodzenia wzroku przez obsługę lub instalatorów;
- 3) adaptory światłowodowe muszą być wyposażone w półprzeźroczyste zaślepki przeciwkurzowe, które pod wpływem oświetlenia toru transmisyjnego źródłem światła widzialnego zmieniają kolor, znacznie ułatwiając identyfikację połączeń bez ryzyka uszkodzenia wzroku osoby z obsługi serwisowej;
- 4) w celu poprawienia obsługi i bezpieczeństwa połączeń adaptory światłowodowe muszą zapewniać kodowanie kolorem oraz zabezpieczenie złączy przed nieautoryzowanym dokonaniem połączenia oraz rozłączenia;
- 5) kolorystyka adapterów połączeniowych będących na wyposażeniu paneli ma umożliwiać identyfikację kabli światłowodowych i być zgodna z **ISO11801 ed.2.2**, tj.:
 - a) dla światłowodów wielomodowych – beżowy lub czarny,
 - b) dla światłowodów jednomodowych PC – niebieski.

Złącza światłowodowe

Złącza światłowodowe będące częścią składową każdego kabla krosowego, preterminowanego oraz pigtaila są kluczowym elementem światłowodowego toru transmisyjnego. Z tego powodu muszą charakteryzować się szeregiem właściwości, które zagwarantują użytkownikowi z jednej strony taki poziom wydajności, który umożliwi obsługę żądanych aplikacji transmisji danych, a z drugiej strony własności mechaniczne zapewniające bezpieczne użytkowanie sieci. Poniżej zestawiono żądane cechy dla złączy światłowodowych:

- 1) zastosowane w panelach złącza muszą charakteryzować się wartościami IL (strata wtrąceniowa) oraz RL (strata odbiciowa) zgodnie z **ISO/IEC 11801 ed. 2.2**. mierzonych metodą zgodnie z **IEC 61300-3-34** dla IL oraz **IEC 61300-3-6** dla RL;
- 2) ferule złączy powinny być ceramiczne, co poprawia mechaniczne własności adaptera (niezawodność, dwukrotnie większa żywotność) oraz poprawia własności optyczne całego połączenia;
- 3) w celu poprawienia obsługi i bezpieczeństwa połączeń złączy światłowodowe muszą zapewniać kodowanie kolorem oraz zabezpieczenie złączy przed nieautoryzowanym dokonaniem połączenia oraz rozłączenia;
- 4) złącza światłowodowe muszą charakteryzować się następującymi parametrami wydajnościowymi:

Tabela 5. Wymagane parametry złączy światłowodowych

Klasyfikacja złączy wg IEC 61753-1	Grade C/2	B _M
Średnie straty wtrąceniowe (IL) [dB] zgodnie z IEC 61300-3-34	≤0,25	≤0,15
Straty wtrąceniowe (RL) [dB] zgodnie z IEC 61300-3-6	≥45 (60)	≥35

4.2.2 Wymagania dotyczące podsystemu okablowania poziomego abonenckiego

Łącza transmisyjne dla poziomego okablowania należy realizować za pomocą okablowania miedzianego pozwalającego uzyskać wydajność klasy EA. W niniejszym podrozdziale przedstawiono szczegółowe wymagania dla tego podsystemu.

4.2.2.1 Miedziane kable instalacyjne

Połączenia poziome miedziane przeznaczone są do obsługi transmisji danych i opierają się na ekranowanym kablu 4P, dla którego szczegółowe wymagania przedstawia *Tabela 6*.

Tabela 6. Wymagane parametry kabla 4P

Kategoria	kat. 6A
Zgodność ze standardami	ISO/IEC 11801 2nd ed.; EN 50173-1 IEC 61156-5 2nd ed.; EN 50288-10-1
Klasyfikacja ogniowa (z uwzględnieniem CPR)	LSZH lub LSFRZH dla stref ochronnych IEC 60332-1 IEC 60754-2 IEC 61034
Ekranowanie	Ustalane na etapie projektowania

4.2.2.2 Moduły przyłączeniowe

Moduły przyłączeniowe stanowią jeden z kluczowych elementów okablowania strukturalnego mających bezpośredni wpływ na wydajność łączy. W związku z powyższym muszą spełniać szereg wymagań gwarantujących zachowanie założeń projektowych:

- 1) w ramach całego systemu okablowania strukturalnego dopuszcza się stosowanie jednego rodzaju modułu we wszystkich zastosowanych platformach;
- 2) moduły muszą jednocześnie umożliwiać wprowadzanie kabla instalacyjnego na wprost (180°) oraz prostopadle (90°), co ma szczególne znaczenie dla gniazd abonenckich, gdzie przestrzeń kablowa jest bardzo ograniczona;
- 3) kategoria zastosowanego miedzianego modułu przyłączeniowego zgodnie z założeniami projektowymi musi spełniać wymagania dla kat. 6A;
- 4) terminacja żył kabla w module musi być wykonana za pomocą technologii IDC (powszechnie uznana za najbardziej niezawodną);
- 5) dla zachowania elastyczności systemu moduły muszą jednocześnie mieć możliwość terminacji żył typu drut w następujących rozpiętościach średnic: AWG 22-24;
- 6) metoda terminacji kabla instalacyjnego w module musi gwarantować niezależność jakości uzyskanego kontaktu od stanu i jakości samego narzędzia terminującego;
- 7) moduły muszą pozwalać na terminację kabla w sekwencji TIA/EIA 568A lub B;
- 8) moduły muszą zapewniać ochronę strefy kontaktu poprzez przytwierdzenie kabla instalacyjnego do obudowy modułu;
- 9) moduły muszą obsługiwać technologię PoE oraz PoE+ (*Power Over Ethernet*);
- 10) żyły kabla instalacyjnego muszą być w obrębie kontaktu IDC unieruchomione, co zapobiega obruszaniu kontaktu; ma to szczególne znaczenie w przypadku zastosowania PoE;
- 11) ekranowanie modułu musi zapewniać ochronę 360°;

- 12) styk ekranowania kabla instalacyjnego z ekranem modułu musi gwarantować przejście o minimalnej impedancji, czyli powierzchnia samego styku powinna być odpowiednio duża.

4.2.2.3 Panele krosowe do obsługi transmisji danych

Panel 1U HD 48 portów

- 1) Panel musi zajmować 1U miejsca w szafie 19”;
- 2) Zagęszczenie portów musi zapewniać obsługę do 48 portów;
- 3) Panel musi umożliwiać kodowanie kolorem, co poprawia walory administracyjne rozwiązań;
- 4) System, w skład którego wchodzi panel, musi zapewniać mechaniczne zabezpieczenie portów przed nieautoryzowanym wpięciem oraz wypięciem złącza do/z gniazda;
- 5) Konstrukcja panelu musi charakteryzować się elastycznością pozwalającą na przyszłe rozbudowy/migracje sieci, tj. panel musi mieć możliwość obsługi:
- a) łączy miedzianych kategorii 6A,
- b) łączy optycznych LC duplex w wersji preterminowanej i spawanej,
- c) jednocześnie dowolnej mieszanki wyżej wymienionych łączy;
- 6) Konstrukcja panelu musi gwarantować możliwość jego obsługi od przodu, co wydatnie usprawnia jego obsługę w sytuacji ograniczonego dostępu do szafy z innych stron;
- 7) Panel musi umożliwiać zaimplementowanie systemu inteligentnego monitorowania portów w dowolnym momencie jego użytkowania bez konieczności rozłączania istniejących połączeń;
- 8) Panel musi posiadać wymienne pola opisowe pozwalające na etykietowanie połączeń. Dodatkowo każdy port musi być ponumerowany;
- 9) Obudowa panelu powinna być w kolorze czarnym/szarym.

Panel 1U 24 porty

- 1) Panel musi zajmować 1U miejsca w szafie 19”;
- 2) Zagęszczenie portów musi zapewniać obsługę do 24 portów;
- 3) Panel musi umożliwiać kodowanie kolorem, co poprawia walory administracyjne rozwiązań;
- 4) System, w skład którego wchodzi panel, musi zapewniać mechaniczne zabezpieczenie portów przed nieautoryzowanym wpięciem oraz wypięciem złącza do/z gniazda;
- 5) Konstrukcja panelu musi charakteryzować się elastycznością pozwalającą na przyszłe rozbudowy/migracje sieci, tj. panel musi mieć możliwość obsługi:
- a) łączy miedzianych kategorii 6A,
- b) łączy optycznych LC duplex w wersji preterminowanej i spawanej,
- c) jednocześnie dowolnej mieszanki wyżej wymienionych łączy;
- 6) Konstrukcja panelu musi gwarantować możliwość jego obsługi od przodu, co wydatnie usprawnia jego obsługę w sytuacji ograniczonego dostępu do szafy z innych stron;
- 7) Panel musi umożliwiać zaimplementowanie systemu inteligentnego monitorowania portów w dowolnym momencie jego użytkowania bez konieczności rozłączania istniejących połączeń;
- 8) Panel musi posiadać wymienne pola opisowe pozwalające na etykietowanie połączeń. Dodatkowo każdy port musi być ponumerowany;
- 9) Obudowa panelu powinna być w kolorze czarnym/szarym.

4.2.2.4 Gniazda PEL

Zaleca się, aby w każdym pomieszczeniu został zainstalowany co najmniej jeden zintegrowany punkt abonencki (PEL – gniazda telekomunikacyjne + gniazda elektryczne). Liczba PEL w każdym pomieszczeniu w budynku powinna zostać określona na etapie przygotowywania przez użytkownika wymagań projektowych. Określając liczbę PEL w pomieszczeniach biurowo-sztabowych, należy kierować się następującą zasadą:

na 8 m² – 1 PEL, gdzie 1 PEL = NxRJ-45 + 2x DATA (230 V)
na 1 pracownika – 1 PEL, gdzie 1 PEL = NxRJ-45 + 2x DATA (230 V)
gdzie N = 3 minimum

Dla każdego PEL przyjmuje się obciążenie mocy max 1000 W.

Powyższe wyliczenia nie dotyczą pomieszczeń innych niż pomieszczenia biurowo-sztabowe, czyli takich pomieszczeń, jak magazyny, sale szkoleniowe itp. W tym przypadku liczba gniazd powinna być określana według specyficznych potrzeb użytkownika. Dotyczy to również doprowadzenia do PEL okablowania światłowodowego.

Gniazda punktów elektryczno-logicznych należy budować w sposób zapewniający łatwy dostęp, na wysokości nie mniejszej niż 30 cm od poziomu podłogi. Gniazda mogą być montowane podtynkowo, natynkowo lub w kanałach elektro-instalacyjnych.

4.2.2.5 Kanały kablowe (podbudowa tras kablowych) i prowadzenie kabli

Kable należy prowadzić w trasach kablowych zrealizowanych w postaci drabin, koryt kablowych metalowych lub PCW, kanałów kablowych i rur instalacyjnych (natynkowo, podtynkowo lub w przestrzeniach pod podłogą techniczną i nad podwieszanym sufitem). Systemy instalacyjne tras kablowych powinny być wyposażone w kształtki kątowe i odgałęźne, łączniki, zaślepki. **Przy doborze przekrojów tras kablowych powinno być uwzględnione 25% rezerwy wolnej przestrzeni.**

W miejscach przejść przez ściany i stropy kable informatyczne powinny być odpowiednio zabezpieczone materiałami/masami ognioodpornymi. Wszystkie przepusty przez przegrody (ściany, stropy) powinny charakteryzować się klasą odporności ogniowej nie niższą, niż klasa odporności ogniowej konkretnej przegrody (EI). Wykonanie i materiały – zgodnie z aprobatą techniczną wyrobu. Przy rozmieszczeniu i prowadzeniu instalacji powinna być zapewniona bezkolizyjność z innymi instalacjami w zakresie określonych odległości i ich wzajemnego usytuowania. Trasy kablowe należy budować z zachowaniem odpowiednich promieni gięcia wiązek kablowych na łukach zgodnie z danymi podanymi w kartach katalogowych kabli.

Zezwala się na prowadzenie okablowania strukturalnego wraz z okablowaniem elektrycznym w tych samych korytach kablowych pod warunkiem zachowania zasad zawartych w polskich normach.

Należy unikać prowadzenia tras kablowych przez pomieszczenia, w których znajdują się urządzenia o dużej mocy (transformatory, silniki), oraz pomieszczenia ze środkami łatwopalnymi. Trasy kablowe należy prowadzić z zachowaniem odpowiednich odległości od źródeł zasilania, takich jak np.:

- 1) wysokonapięciowe oświetlenie;
- 2) przewody elektryczne 5 kVA lub więcej;
- 3) transformatory i silniki.

Dla sieci teleinformatycznych do klauzuli „ZASTRZEŻONE” nie stosuje się oznakowania tras kablowych (wskazującego sieć, w której przetwarzane są informacje niejawne).

4.2.2.6 Wymagania dotyczące kabli połączeniowych i krosowych

Kable połączeniowe i krosowe powinny być dostarczone przy budowie każdej sieci strukturalnej. Ich długość (od 0,5 m do 5 m) powinna być uzgodniona z Użytkownikiem i Inwestorem na etapie wykonywania dokumentacji projektowej. Mogą być wykorzystywane tylko kable typu „linka”. Użyte kable bezwzględnie muszą przewyższać klasę budowanego okablowania, a ponadto:

- 1) muszą być wykonane z tworzywa bezhalogenowego (LSOH);
- 2) powinny pochodzić od tego samego producenta co budowany system okablowania strukturalnego.

Przyjmuje się zasadę, że w ramach inwestycji budowy okablowania strukturalnego dostarcza się kable krosowe i połączeniowe w ilościach 66% całkowitej ilości gniazd RJ-45, w PEL dla kabli połączeniowych i w panelach krosowych dla kabli krosowych. Dla kabli optycznych ilości każdorazowo należy specyfikować na etapie projektowym w zależności od specyficznych potrzeb użytkowych.

Przyjęto oznaczenia kolorystyczne (piktogramy) patchcordów – dla użytkowników:

- | | |
|-------------------|-----------|
| 1) ASK sieć jawna | szary |
| 2) ST MILNET-Z | niebieski |
| 3) ST MILNET-I | żółty |
| 4) CCTV/Domofony | zielony |
| 5) SKD | brąz |
| 6) I&HAS | fiolet |
| 7) SSP | czerwony |
| 8) inne | biały |

4.3 Administracja, etykietowanie

Wszystkie kable powinny być oznaczone numerycznie, w sposób trwały, zarówno od strony gniazda, jak i od strony szafy montażowej zgodnie ze standardem **TIA-606-B** oraz **ISO/IEC TR14763-2-1**. Te same oznaczenia należy umieścić w sposób trwały na gniazdach sygnałowych w punktach przyłączeniowych użytkowników oraz na panelach.

Powykonawczo należy sporządzić dokumentację instalacji kablowej zawierającej trasy kablowe i rozmieszczenie punktów przyłączeniowych w pomieszczeniach zgodnie ze stanem rzeczywistym według wytycznych określonych w 4.5. Do dokumentacji należy dołączyć raporty z pomiarów torów sygnałowych.

4.4 Wymagania gwarancyjne

Całość rozwiązania ma być objęta jednolitą, spójną, minimum 25-letnią gwarancją systemową producenta, obejmującą całą część transmisyjną wraz z kablami krosowymi i innymi elementami dodatkowymi. Gwarancja ma być udzielona przez producenta bezpośrednio klientowi końcowemu.

Gwarancja systemowa musi obejmować:

- 1) gwarancję produktową (producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź minimum 25-letniego czasu eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione);

- 2) gwarancję parametrów łącza/kanału (producent zagwarantuje, że łącze stałe bądź kanał transmisyjny zbudowane z jego komponentów przez okres minimum 25 lat będą charakteryzowały się parametrami transmisyjnymi przewyższającymi wymogi stawiane przez normę **ISO/IEC11801 2nd edition:2002** dla klasy E_A).

4.5 Odbiory

Warunkiem koniecznym dla odbioru końcowego instalacji przez Inwestora jest uzyskanie gwarancji systemowej producenta potwierdzającej weryfikację wszystkich zainstalowanych torów na zgodność parametrów z wymaganiami norm Klasy E_A (kategorii 6_A zgodnie z normami referencyjnymi). Mierniki użyte w procesie pomiarowym muszą uzyskać aprobatę producenta systemu okablowania i posiadać aktualny certyfikat wzorcowania.

Wykonanie dokumentacji powykonawczej Dokumentacja powykonawcza musi zostać wykonana i przekazana Inwestorowi. Musi ona zawierać między innymi:

- 1) raporty z pomiarów dynamicznych okablowania;
- 2) rzeczywiste trasy prowadzenia kabli transmisyjnych poziomych;
- 3) oznaczenia poszczególnych szaf, gniazd, kabli i portów w panelach krosowych;
- 4) lokalizację przebiegów przez ściany i podłogi;
- 5) raporty pomiarowe wszystkich torów transmisyjnych należy zawrzeć w dokumentacji powykonawczej i przekazać inwestorowi przy odbiorze inwestycji. Drugą kopię pomiarów (dokumentacji powykonawczej) należy przekazać producentowi okablowania w celu udzielenia inwestorowi (Użytkownikowi końcowemu) bezpłatnej gwarancji.
- 6) oddzielna kopia dokumentacji powykonawczej musi być przekazana do Działu Informatyki (wersja papierowa i elektroniczna, część rysunkowa w formatach PDF i DWG).

5 WYMAGANIA DOTYCZĄCE KANALIZACJI TELETECHNICZNEJ I PROWADZENIA KABLI ZEWNĘTRZNYCH

Kanalizację teletechniczną należy budować zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 26 maja 2023 r. w sprawie warunków technicznych, jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie przy wykorzystaniu rur o średnicy 110 mm. Liczba otworów kanalizacji będzie ustalana na etapie projektowania. Typ i rodzaj studni kablowych należy stosować w zależności od miejsca posadowienia i dowiązania do istniejącej kanalizacji. Projekty dotyczące kanalizacji i kabli należy uzgodnić z Sekcją Infrastruktury Teleinformatycznej (SIT) Działu Informatyki (DIN).

Kable zewnętrzne wieloparowe miedziane i optyczne należy układać bezpośrednio w kanalizacji teletechnicznej oraz należy oznaczyć je według poniższych wymagań w każdej studni oraz po wejściu do budynku.

Po zakończeniu robót budowlanych branży telekomunikacyjnej (budowa, rozbudowa, demontaż) należy przeprowadzić geodezyjną inwentaryzację powykonawczą, zgodnie z obowiązującymi przepisami.

5.1 Telekomunikacyjne kable miedziane

- 1) Kable miejscowe o budowie czwórkowej uszczelnione wzdłużne wykorzystywane są do połączeń stacji abonenckich z centralą w obrębie kampusu (XzTKMXpw). Należy je układać w kanalizacji kablowej. Zakończenia kabla: przełącznica główna (PG), rozłączne LSA (krone), zewnętrzna szafka kablowa (SK) łączówki LSA (krone) wypełnione żelam, z zachowaniem paroszczelności SK. W komorze kablowej należy przejść na kabel stacyjny.
- 2) Kable stacyjne (budynkowe) – o powłoce niepalnej lub uniepalnionej zgodnie z wymaganiami opisanymi w normach. Kable w szafach RACK zaterminować na panelach ISDN.
- 3) Zachować ciągłość uziemienia w kablach miejscowych.

5.2 Przywieszki identyfikacyjne

Przywieszki identyfikacyjne muszą mieć wielkość 80x35 mm oraz zostać zalaminowane, a otwory do mocowania muszą być umieszczone poza obszarem identyfikacyjnym kabla.

Kable miedziane – kolor tła zielony, napisy czarne

Rys. 2. Przywieszka identyfikacyjna kabla miedzianego

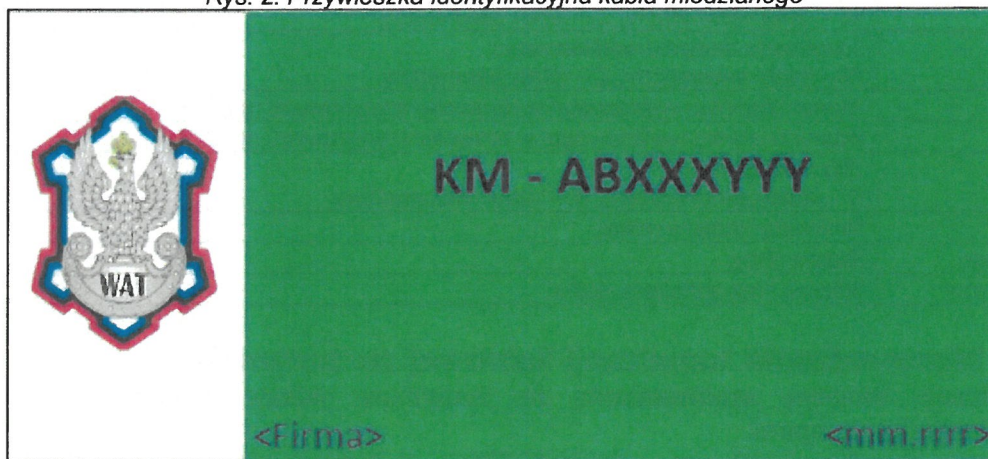


Tabela 7. Oznaczenia w przywieszce identyfikacyjnej kabla miedzianego

Oznaczenie	Znaczenie i dopuszczalne wartości
KM	Kabel miedziany
A	Lokalizacja budynku wyjściowego: W – teren wewnętrzny, Z – teren zewnętrzny
B	Lokalizacja budynku wejściowego: W – teren wewnętrzny, Z – teren zewnętrzny
XXX	Numer budynku wyjściowego w formacie trzycyfrowym, np. 022
YYY	Numer budynku wejściowego w formacie trzycyfrowym, np. 029
<Firma>	Nazwa firmy
<mm.rrrr>	Miesiąc i rok położenia kabla

Kable światłowodowe – kolor tła niebieski, napisy czarne

Rys. 3. Przywieszka identyfikacyjna kabla światłowodowego

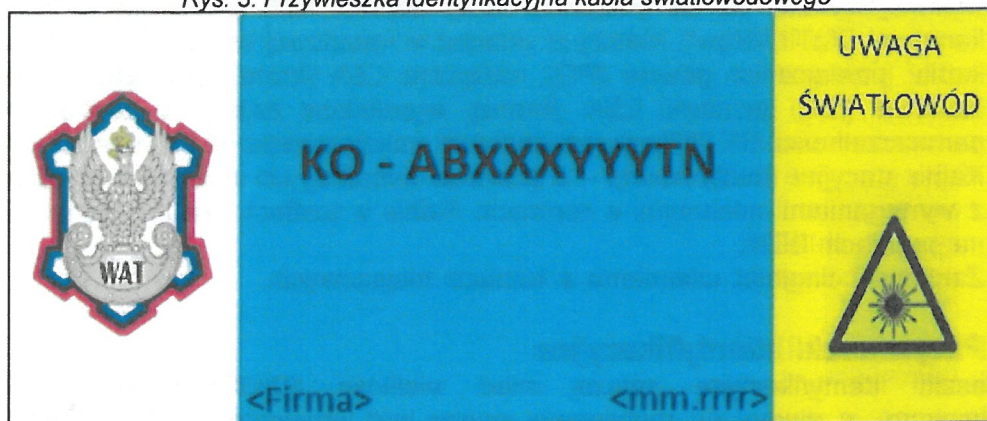


Tabela 8. Oznaczenia w przywieszce identyfikacyjnej kabla światłowodowego

Oznaczenie	Znaczenie i dopuszczalne wartości
KO	Kabel światłowodowy (optyczny)
A	Lokalizacja budynku wyjściowego: W – teren wewnętrzny, Z – teren zewnętrzny
B	Lokalizacja budynku wejściowego: W – teren wewnętrzny, Z – teren zewnętrzny
XXX	Numer budynku wyjściowego w formacie trzycyfrowym, np. 022
YYY	Numer budynku wejściowego w formacie trzycyfrowym, np. 029
T	Typ światłowodu: S – kabel jednomodowy, M – kabel wielomodowy
1	Nr kolejny kabla w relacji
<Firma>	Nazwa firmy
<mm.rrrr>	Miesiąc i rok położenia kabla

5.3 Wprowadzenia kanalizacji kablowej do budynków

Kanalizację kablową wprowadzoną do budynków należy uszczelnić zgodnie z poniższymi wymogami:

- 1) rury kanalizacji 110 mm – uszczelki TDUX, Jackmoon lub równoważne;
- 2) rury kanalizacji 110 mm z kablami prowadzonymi bezpośrednio w rurze – uszczelki TDUX, Jackmoon lub równoważne;
- 3) rury HDPE 40 mm z kablami światłowodowymi – uszczelki Jackmoon lub równoważne.

Ostatni (pierwszy) odcinek instalacyjny

Wprowadzenie kabli światłowodowych do budynków może być wykonane jako:

- 1) wprowadzenie kablem liniowym w powłocę niepalnej – ostatni (pierwszy) odcinek instalacyjny powinien być wykonany z kabla o powłocę nierozprzestrzeniającej ognia, bezhalogenowej;
- 2) wprowadzenie kablem liniowym w powłocę palnej polietylenowej – odcinek instalacyjny (wewnątrz budynku) powinien być zabezpieczony przed bezpośrednim dostępem płomieni i rozprzestrzenianiem ognia poprzez umieszczenie tego odcinka w rurach osłonowych z materiałów nierozprzestrzeniających ognia, bezhalogenowych. Końce rur powinny być odpowiednio uszczelnione materiałem niepalnym.

Wejście z kablami do budynku należy realizować tylko poprzez przyłącze kablowe.
W przypadku braku takiego przyłącza należy je bezwzględnie wykonać.

6 WYMAGANIA W ZAKRESIE SERWEROWNI BUDYNKOWYCH / GPD / PPD

W celu zapewnienia wymaganego poziomu bezpieczeństwa serwerowni budynkowych / GPD / PPD należy spełnić między innymi następujące warunki:

- 1) wyposażenia w środki zabezpieczenia elektronicznego, systemu kontroli dostępu, I&HAS, CCTV;
- 2) monitorowania parametrów środowiskowych przez zarządzalne listwy zasilające;
- 3) wyposażenia w redundantną klimatyzację;
- 4) pomieszczenie powinno być bez okien. W przypadku, kiedy pomieszczenie posiada okna powinny zostać wykonane zabezpieczenia mechaniczne (kraty) oraz pomieszczenie musi zostać zabezpieczone przed narażeniem urządzeń na oddziaływanie słoneczne;
- 5) wyposażenia technicznego;
- 6) wyposażenia bezpieczeństwa pożarowego;
- 7) certyfikowanej stolarki (drzwi z futryną) według normy **PN-EN-1627**.

7 WYMAGANIA W ZAKRESIE ZASILANIA SIECI TELEINFORMATYCZNYCH

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa, prawidłowej eksploatacji i działania systemów teleinformatycznych, urządzeń IT oraz przechowywanych w nich danych wymagany jest odpowiedni dobór sposobu zasilania i uziemienia sieci komputerowej.

Instalacja oddzielonej sieci zasilania elektrycznego. W budowanych sieciach teleinformatycznych zasilanie i uziemienie sieci teleinformatycznych realizuje się poprzez budowę takiej instalacji elektrycznej, która jest systemem wydzielonym z ogólnej instalacji elektrycznej. Dla takiej sieci zasilającej:

- 1) bilans mocy budowanej instalacji elektrycznej musi uwzględniać już eksploatowane instalacje elektryczne;
- 2) obwody elektryczne oraz szafy teleinformatyczne muszą być zasilane z wydzielonych pól tablic rozdzielczych;
- 3) gniazda odbiorcze muszą być zaopatrzone w klucze pozwalające na podłączanie tylko konkretnych urządzeń;
- 4) instalacja powinna być wybudowana zgodnie z obowiązującymi polskimi normami w zakresie instalacji elektrycznych.

Niniejszy dokument nie określa wymogów dotyczących doboru/budowy zasilania awaryjnego. Powyższe jest określane przez Użytkowników na etapie wykonywania założeń projektowych i zależy od specyfiki i przeznaczenia obiektu.

W nowobudowanych i remontowanych serwerowniach, wszystkie baterie dedykowane dla UPS należy instalować w odrębnych pomieszczeniach.

8 WYMAGANIA W ZAKRESIE URZĄDZEŃ AKTYWNYCH

W celu ujednolicenia sieciowego sprzętu aktywnego w ASK WAT oraz wykonywania kolejnych podłączeń do nowego szkieletu sieci komputerowej należy wykorzystywać wyłącznie urządzenia spełniające poniższe założenia.

Umożliwi to Działowi Informatyki nadzorowanie i zarządzanie zarówno ruchem sieciowym, jak i bezpieczeństwem sieci komputerowej. W przypadku wątpliwości co do planowanego sprzętu sieciowego wymagana jest konsultacja z Działem Informatyki, który podejmuje ostateczną decyzję.

8.1 Wymagania ogólne dla urządzeń i oprogramowania sieciowego

- 1) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski – podczas dostawy należy dołączyć do faktury oświadczenia producenta sprzętu i oprogramowania (lub jego polskiego przedstawicielstwa) o spełnieniu tego wymogu.
- 2) Całość dostarczanego sprzętu musi być nowa (wyprodukowaną nie wcześniej niż 6 miesięcy przed dostawą), nieużywana we wcześniejszych projektach – wraz z dostawą należy dostarczyć oświadczenie producenta (lub jego polskiego przedstawicielstwa) potwierdzające datę produkcji urządzeń.
- 3) Całość sprzętu i oprogramowania musi być dostarczona do Zamawiającego. Wszystkie elementy systemu muszą ze sobą współpracować i umożliwiać pełną funkcjonalność wyszczególnioną w „Opisie przedmiotu zamówienia” lub „Programie Funkcjonalno-Użytkowym”.
- 4) Dostęp do aktualnych sterowników urządzenia, realizowany poprzez podanie identyfikatora klienta lub modelu urządzenia lub numeru seryjnego urządzenia, na dedykowanej przez producenta stronie internetowej.
- 5) W przypadku zaoferowania przez Wykonawcę urządzenia, dla którego dostęp do aktualnych sterowników urządzenia wymaga wykupienia kontraktu serwisowego producenta, po stronie Wykonawcy istnieje obowiązek uwzględnienia go w dostawie. Kontrakt serwisowy musi pokrywać się z okresem gwarancyjnym urządzenia.
- 6) Obowiązek, o którym mowa w pkt. 5, nie istnieje, jeśli wskazano inaczej w „Opisie przedmiotu zamówienia” lub „Programie Funkcjonalno-Użytkowym”.

8.2 Warunki gwarancji i wsparcia technicznego dla sprzętu i oprogramowania sieciowego

- 1) Całość dostarczonego sprzętu musi być objęta gwarancją producenta opartą o świadczenia gwarancyjne producenta sprzętu, niezależne od statusu partnerskiego Wykonawcy przez okres min. 36 miesięcy.
- 2) Serwis gwarancyjny musi być oparty na świadczeniach gwarancyjnych producenta.
- 3) Na dostarczany sprzęt musi być udzielona min. 36 miesięczna gwarancja, oparta na gwarancji producenta rozwiązania; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu przez Wykonawcę; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć 4 godzin; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu 2 dni roboczych od momentu zgłoszenia usterki; Serwis musi być

- świadczony przez 8 godzin na dobę przez 5 dni w tygodniu. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Zaproponowany pakiet serwisowy musi zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (a nie tylko u Wykonawcy) przez cały okres trwania gwarancji.
- 4) W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 10 dni od momentu zgłoszenia usterki.
 - 5) Zamawiający w zaproponowanych pakietach serwisowych producenta musi otrzymać dostęp do pomocy technicznej producenta (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Zamawiającego.
 - 6) Wszystkie dostarczane moduły (np. typu SFP) muszą pochodzić od producenta urządzeń sieciowych i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu.

8.3 Urządzenia do sieci resortowych

Wykazy corocznie publikowane są przez Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni na stronie:

<https://www.wojsko-polskie.pl/woc/wykaz-obowiazujacych-standardow/>

Jeżeli na wykazie brak jest urządzeń aktywnych, należy zwrócić się do Działu Informatyki. W sieciach resortowych nie ma możliwości dołączenia urządzeń, które nie zostały dopuszczone do użytku.

8.4 Urządzenia do Kampusowej Sieci Bezprzewodowej (KSB)

W Wojskowej Akademii Technicznej uruchomiono Kampusową Sieć Bezprzewodową (KSB) zarządzaną i rozbudowywaną przez Dział Informatyki. Rozbudowa KSB może być realizowana wyłącznie przy współdziałaniu z Działem Informatyki. Poniższe wytyczne należy traktować jako specyfikację techniczno-użytkową – wymagania minimalne.

8.4.1 Wymaganie ogólne

W przypadku urządzeń sieci bezprzewodowej wykonawca musi zapewnić pełny roaming użytkowników w obrębie całej sieci bezprzewodowej oraz zapewnić pełen automatyzm związany z planowaniem radiowym (tj. dobieranie kanałów, separacji, ich szerokości oraz mocy sygnału dla sieci o tych samych SSID). Z uwagi na stosowanie przez Zamawiającego posiadanego narzędzia Air Marshal służącego do ochrony sieci bezprzewodowych, oferowane rozwiązanie musi tak współpracować z obecnie posiadanym rozwiązaniem, aby możliwa była nadal ochrona kampusowej sieci bezprzewodowej z użyciem narzędzia Air Marshal.

8.4.2 Przyjęty standard

Powyższe wymagania spełniają urządzenia Meraki i przyjęto je jako standard w KSB. Wszystkie urządzenia Meraki muszą być podpięte do panelu centralnego WAT na aktywnym koncie zarządzanym przez Dział Informatyki.

Wskazuje się wymóg dla licencji (subskrypcji) na okres min. 5 lat, przy czym licencja ta jest dodawana do systemu w modelu licencjonowania z współterminacją (co-term).

Oznacza to, że nowe licencje przedłużają okres licencji dla wszystkich urządzeń w KSB.

8.4.3 Dopuszczone urządzenia i akcesoria sieciowe do KSB

- 1) **Access Point Meraki MR46** w konfiguracji:
 - a) MR46-HW – Meraki MR46 Wi-Fi 6 Indoor AP,
 - b) LIC-ENT-5YR – Meraki MR Enterprise License, 5YR
lub model wyższy/lepszy, tj. o lepszych parametrach technicznych i odpowiadająca temu modelowi licencja o terminie nie krótszym niż wskazany;
- 2) **Access Point Meraki MR36** w konfiguracji:
 - a) MR36-HW – Meraki MR36 Wi-Fi 6 Indoor AP,
 - b) LIC-ENT-5YR – Meraki MR Enterprise License, 5YR
lub model wyższy/lepszy, tj. o lepszych parametrach technicznych i odpowiadająca temu modelowi licencja o terminie nie krótszym niż wskazany;
- 3) **Przełącznik sieciowy Meraki MS120 8p** w konfiguracji:
 - a) MS120-8FP-HW – Meraki MS120-8FP 1G L2 Cloud Managed 8x GigE 124W PoE Switch,
 - b) LIC-MS120-8FP-5YR – Meraki MS120-8FP Enterprise License and Support, 5 Year,
 - c) MA-PWR-CORD-EU – Meraki AC Power Cord for MX and MS (EU Plug)
lub model wyższy/lepszy, tj. o lepszych parametrach technicznych i odpowiadająca temu modelowi licencja o terminie nie krótszym niż wskazany;
- 4) **Przełącznik sieciowy Meraki MS120 24p** w konfiguracji:
 - a) MS120-24P-HW – Meraki MS120-24P 1G L2 Cld -Mngd 24x GigE 370W PoE Switch,
 - b) LIC-MS120-24P-5YR – Meraki MS120-24P Enterprise License and Support, 5 Year,
 - c) MA-PWR-CORD-EU – Meraki AC Power Cord for MX and MS (EU Plug)
lub model wyższy/lepszy, tj. o lepszych parametrach technicznych i odpowiadająca temu modelowi licencja o terminie nie krótszym niż wskazany;
- 5) **Meraki 1000Base SX Multi-Mode** (P/N: MA-SFP-1GB-SX) lub model wyższy/lepszy, tj. o lepszych parametrach technicznych;
- 6) **1000BASE-SX SFP transceiver module, MMF, 850nm, DOM** (P/N: GLC-SX-MMD=) lub model wyższy/lepszy, tj. o lepszych parametrach technicznych;
- 7) **Montaż i konfiguracja rozwiązania** – wymagane podłączenie do istniejącej instalacji, w tym:
 - a) montaż nowych AP (poz. 1-6),
 - b) rozwiązanie musi zostać zintegrowane z oprogramowaniem Cisco ISE posiadany przez Zamawiającego oraz dołączone do istniejącej instalacji bazującej na ww. urządzeniach,
 - c) wykonanie dokumentacji powdrożeniowej,
 - d) architektura rozwiązania musi umożliwiać dalszą rozbudowę.

8.4.4 Wymagania dla firmy odpowiadającej za montaż i konfigurację

- 1) w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie: wykonał co najmniej jedno zamówienie obejmujące swym zakresem dostawę wraz z usługą uruchomienia i serwisu gwarancyjnego realizowanego w okresie min. 12 miesięcy rozwiązań sieci bezprzewodowej Cisco Meraki, o wartości nie mniejszej niż 800 000,00 zł brutto.

- 2) skieruje do realizacji usługi co najmniej 1 (jedną) osobę posiadającą kwalifikacje certyfikowanego inżyniera Cisco CCIE (z ang. Cisco Certified Internetworking Expert) w specjalności Security i Data Center z co najmniej dwuletnim doświadczeniem w obszarze routerów i przełączników typu SDN Cisco ACI oraz bezpieczeństwa ruchu sieciowego opartego o rozwiązania Cisco.

8.5 Urządzenia do Akademickiej Sieci Komputerowej

8.5.1 Przyjęty standard

Przyjętym standardem dla aktywnych urządzeń sieciowych w Akademickiej Sieci Komputerowej WAT są urządzenia Cisco.

Zgodnie z art. 99 ust. 5 Prawo Zamówień Publicznych w niektórych przypadkach pozwala na wskazanie wymaganych urządzeń, oczywiście przy zachowaniu, iż nowe urządzenia Cisco są rozbudową istniejącej infrastruktury kampusowej, zakupionej w poprzednich przetargach. Ze względu na wymagania licencyjne, gwarancyjne oraz zgodność komunikacji między urządzeniami i systemem monitorującym zamawiane produkty są wskazane wprost lub z jednoznacznym wskazaniem przeznaczenia. Rozwiązanie to jest preferowane ze względu na istniejącą architekturę teleinformatyczną obecnie funkcjonującą w WAT, a tym samym:

- 1) przystosowanie środowiska informatycznego pod to rozwiązanie (narzędzia sieciowe, stosowane specjalistyczne oprogramowanie, w tym monitoring i integracja Cisco ISE);
- 2) przeszkolenie administratorów systemów i zwykłych użytkowników;
- 3) opracowanie zasad organizacyjnych.

8.5.2 Równoważność

Jeżeli wykonawca zaproponuje inne rozwiązanie niż istniejące o parametrach nie gorszych niż dla wyspecyfikowanych urządzeń (kryteriami równoważności) musi zapewnić pełne wdrożenie oferowanego rozwiązania wraz z wymaganymi licencjami, przeszkoleniem użytkowników i administratorów systemu oraz zapewnić pełną współpracę z używanym obecnie środowiskiem informatycznym oraz systemem monitoringu.

Urządzenia, które nie będą spełniały opisanych kryteriów lub nie będą zgodne z niniejszymi warunkami z przyczyn bezpieczeństwa mogą nie zostać podłączone do sieci kampusowej.

W celu uniknięcia jakichkolwiek nieporozumień przed przystąpieniem do realizacji należy każdorazowo uzgadniać (na każdym etapie: koncepcja, projekt, wykonanie):

- 1) infrastrukturę teletechniczną z Sekcją Infrastruktury Teleinformatycznej Działu Informatyki;
- 2) urządzenia aktywne z Sekcją Infrastruktury Usługowej Działu Informatyki.

8.5.3 Routery

8.5.3.1 Zakres zamówienia

- 1) dostawa urządzeń, obejmująca sprzedaż i dostarczenie przez Wykonawcę do Lokalizacji Zamawiającego urządzeń wraz z dokumentacją i oprogramowaniem;
- 2) urządzenia będą objęte gwarancją na urządzenia i wsparciem technicznym na oprogramowanie przez min. okres 36 miesięcy od dnia podpisania protokołu odbioru dostawy.

8.5.3.2 Wymagania Ogólne

- 1) Wykonawca wraz z urządzeniami dostarczy zestaw montażowy rack tj. wszystkie niezbędne elementy konieczne do ich montażu w lokalizacjach Zamawiającego, w szczególności: śrubki, nakrętki koszykowe, kable zasilające, szyny montażowe, itp.;
- 2) urządzenia muszą pochodzić od tego samego producenta oraz być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale”, „end-of-life” oraz „end-of-support” producenta;
- 3) urządzenia muszą posiadać najnowszą dostępną stabilną wersję oprogramowania;
- 4) nie dopuszcza się oferowania urządzeń, dla których producent nie udostępnia już najnowszej wersji oprogramowania / systemu operacyjnego.

8.5.3.3 Szczegółowe wymagania dla każdego z Urządzeń

- 1) musi posiadać co najmniej 12 portów, z czego przynajmniej 4 z nich można ustawić w tryb 1GE lub 10 GE, a 8 w tryb 1GE. Interfejsy 1GE muszą być definiowane przez wkładki SFP, a interfejsy 10GE przez wkładki optyczne SFP+. W przypadku urządzeń o niekonfigurowalnych przepustowościach portów, urządzenie powinno być wyposażone minimum w 4 porty 10GE i 10 portów 1GE;
- 2) musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR;
- 3) musi mieć możliwość redundancji zasilania oraz warstwy kontrolnej ze wsparciem NSF i SSO – dopuszczalna realizacja za pomocą zdublowanych modułów kontroli albo przez zapewnienie możliwości jednoczesnego uruchomienia dwóch instancji systemu operacyjnego;
- 4) musi być wyposażone w co najmniej 16 GB pamięci RAM;
- 5) musi umożliwiać rozbudowę pamięci RAM do co najmniej 64 GB RAM;
- 6) musi być wyposażone w pamięć o pojemności co najmniej 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych;
- 7) musi obsługiwać co najmniej 3 500 000 prefiksów w tablicach routingu IPv4 lub co najmniej 2 000 000 prefiksów w tablicy routingu IPv6;
- 8) musi oferować sumaryczną wydajność dla pakietów 1400B na poziomie przynajmniej 19 Gbps dla ruchu IPv4;
- 9) musi oferować sumaryczną wydajność dla pakietów szyfrowanych 1400B na poziomie przynajmniej 15Gbps dla ruchu IPv4;
- 10) musi być przystosowane do montażu w szafie 19", obudowa wykonana z metalu;
- 11) musi posiadać zasilacz przystosowany do zasilania prądem naprzemiennym 230V.

8.5.3.4 Funkcje oprogramowania

- 1) musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6;
- 2) musi posiadać wsparcie dla MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN);
- 3) musi być w stanie obsłużyć co najmniej 6000 instancji VRF (Virtual Route Forwarding);

- 4) musi mieć możliwość podłączenia wewnętrznym logicznym interfejsem wirtualny router (VRF) z globalną tablicą routingu;
- 5) musi posiadać ochronę warstwy zarządzającej (Control Plane Policing);
- 6) musi obsługiwać co najmniej 4000 ACL (Access Control Lists) z 50 000 wpisów ACE (Access Control Entries);
- 7) musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2;
- 8) musi obsługiwać RPF (Reverse Path Forwarding);
- 9) musi obsługiwać zarządzanie ruchem (QoS):
 - a) minimum 16000 kolejek per system,
 - b) hierarchiczne polityki QoS,
 - c) 3 poziomy hierarchii,
 - d) dwie kolejki priorytetowe LLQ per polityka;
- 10) musi mieć możliwość definicji własnych sygnatur aplikacji, na bazie których nastąpi klasyfikacja ruchu do kolejki QoS;
- 11) musi obsługiwać funkcjonalność sFlow lub odpowiednik (J-Flow, NetFlow);
- 12) musi posiadać funkcjonalność VRRP lub odpowiednika;
- 13) musi umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
- 14) musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS);
- 15) urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do urządzenia i uruchomiona;
- 16) urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów;
- 17) urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem co najmniej AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.

8.5.3.5 Wyposażenie urządzenia:

- 1) musi być wyposażony w licencję umożliwiającą skorzystanie z przepustowości 1000/1000Mbps (sumarycznie 2Gbps) dla ruchu szyfrowanego;
- 2) musi być wyposażony w licencję umożliwiającą wykorzystanie pełnej wydajności dla ruchu nieszyfrowanego w standardowym trybie pracy urządzenia.

8.5.3.6 Oprogramowanie/funkcjonalności dla trybu pracy SD-WAN

- 1) szyfrowanie wszystkich łączy WAN z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łączy spełniające wymagania aplikacji zdefiniowane w polityce
 - a) bezpieczne połączenie WAN lokalizacji, wykorzystując w tym celu dowolną kombinację połączeń przez sieć transportową (IP VPN), jak też opcjonalnie sieci publiczne (Internet),
 - b) aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy lokalizacjami, odpowiednio sterując ruchem zależnie od aktualnych warunków,
 - c) elastyczne tworzenie topologii (gwiazda, częściowa lub pełna kratę, punkt-punkt) per segment,
 - d) monitorowanie wydajności wszystkich łączy systemu,

- e) równoważenie obciążenia poszczególnych łącz (per sesja):
 - statyczne (active/standby i active/active równoważne i ważne),
 - dynamiczne oparte o monitorowanie jakości w danym czasie,
 - f) redundancja active-active urządzeń na poziomie zakończenia usługi w każdej lokalizacji (jedno urządzenie CE obsługujące łącze podstawowe, drugie urządzenie CE obsługujące łącza podstawowe i zapasowe);
- 2) funkcjonalności z zakresu bezpieczeństwa:
- a) szyfrowanie wszystkich połączeń co najmniej AES256,
 - b) funkcja skrótu co najmniej SHA-2,
 - c) uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared),
 - d) obsługa list kontroli dostępu (ACL),
 - e) segmentacja sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa co najmniej 4-ech segmentów,
 - f) obsługa translacji adresów NAT/PAT i NAT Traversal – wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji – ruch taki powinien być translowany i lokalnie wychodzić do Internetu,
 - g) możliwość segmentacji routera na 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN,
 - h) funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall),
 - i) musi mieć możliwość rozszerzenia o funkcjonalność umożliwiającą agregację tuneli VPN z komputerów użytkowników;
- 3) polityki jakości obsługi aplikacji:
- a) możliwość definicji polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach – w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki,
 - b) monitorowanie jakości dostępu do usług chmurowych typu SaaS (co najmniej Google Apps, Office365, Dropbox) i IaaS (co najmniej AWS, Azure) z możliwością optymalizacji dostępu do nich – system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi;
- 4) mechanizmy zapewnienia jakości ruchu (QoS):
- a) obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma,
 - b) kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu,
 - c) mechanizm tail-drop i RED (Random Early Detect),
 - d) oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu,
 - e) mechanizm odzyskiwania utraconych pakietów przez dodanie dodatkowych nadmiarowych danych do transmisji. Mechanizm powinien mieć możliwość skonfigurowania aplikacji, dla których jest aplikowany oraz możliwość

- złączenia się (wysyłania nadmiarowych danych) tylko, gdy warunki sieciowe ulegną degradacji;
- 5) obsługa protokołów routingu dynamicznego:
 - a) OSPFv2 (także na portach LAN),
 - b) BGP,
 - c) BFD,
 - d) Multicast z obsługą replikacji w poszczególnych węzłach sieciowych (w celu uniknięcia replikacji u źródła);
 - 6) obsługa protokołów i funkcjonalności sieciowych:
 - a) 802.1q,
 - b) VRRP,
 - c) Serwer DHCP,
 - d) SSHv2,
 - e) SNMP v2c, v3,
 - f) NTP z uwierzytelnieniem,
 - g) Syslog;
 - 7) rozwiązanie ma opierać się o centralny kontroler, routery CE uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi;
 - 8) interfejs kontrolera musi zapewniać:
 - a) graficzny interfejs konfiguracyjny,
 - b) obsługę API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler; dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML,
 - c) obsługę RBAC (możliwość zróżnicowania ról administratorów w zakresie brak dostępu / tylko odczyt / pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa),
 - d) zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych,
 - e) wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu,
 - f) zarządzanie oraz diagnostyka z poziomu GUI oraz CLI,
 - g) konfiguracja urządzeń oparta o wzorce konfiguracyjne,
 - h) dostarczone z wszystkimi niezbędnymi licencjami umożliwiającymi uruchomienie wymienionych funkcjonalności, obejmującymi możliwość instalacji kontrolera SD-WAN jako maszyny (maszyn) wirtualnych pracujących z wirtualizatorem VMWare ESXi.

8.5.4 Przełączniki dostępowe Typ 1

- 1) rodzaj urządzenia:
 - a) przełącznik Gigabit Ethernet wyposażony w 24/48 portów 10/100/1000BaseT,
 - b) porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH), 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR,) lub SFP28 (co najmniej 25GBASE-SR, 25GBASE-SL, 25GBASE-LR) zależnie od potrzeb Zamawiającego,
 - c) w razie potrzeby można zastosować przełącznik zapewniający PoE+;

- 2) wyposażenie:
 - a) slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
 - 25G/10G SFP28,
 - 1G SFP,
 - 10G SFP+,
 - b) porty SFP/SFP+/QSFP możliwe do obsadzenia wkładkami zależnie od potrzeb:
 - porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,
 - porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
 - porty SFP28 – wkładki 25Gigabit Ethernet w tym SFP-25G-SR-S, SFP-25G-SL, SFP-10/25G-CSR-S, SFP-10/25G-LR-S, FP-10/25G-LR-I, kable DAC i AOC;
- 3) możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
 - a) przepustowość w ramach stosu – 480Gb/s,
 - b) 8 urządzeń w stosie,
 - c) zarządzanie poprzez jeden adres IP,
 - d) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
 - e) możliwość współdzielenia mocy zasilaczy (grupy do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (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);
- 4) zasilanie i chłodzenie:
 - a) zasilacz prądem naprzemiennym 230V, możliwość instalacji zasilacza redundantnego,
 - b) redundantne i wymienne moduły wentylatorów,
 - c) przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności);
- 5) parametry wydajnościowe:
 - a) szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
 - b) bufor pakietów – co najmniej 16 MB,
 - c) pamięć DRAM – co najmniej 8 GB,
 - d) pamięć flash – co najmniej 16 GB,
 - e) obsługa:
 - 4.000 identyfikatorów sieci VLAN,
 - 32.000 adresów MAC,
 - 24.000 tras IPv4,
 - 16.000 tras IPv6;
- 6) obsługa protokołu NTP;
- 7) obsługa IGMPv1/2/3 i MLDv1/2 Snooping;

- 8) przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a) IEEE 802.1w Rapid Spanning Tree,
 - b) Per-VLAN Rapid Spanning Tree (PVRST+),
 - c) IEEE 802.1s Multi-Instance Spanning Tree,
 - d) Obsługa 128 instancji protokołu STP;
- 9) obsługa protokołu LLDP i LLDP-MED.;
- 10) obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego;
- 11) możliwość uruchomienia funkcji serwera DHCP;
- 12) mechanizmy związane z bezpieczeństwem sieci:
 - a) wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
 - b) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
 - c) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
 - d) obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
 - e) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
 - f) możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
 - g) możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
 - h) obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
 - i) zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
 - j) możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
 - k) obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
 - l) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
 - m) wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
 - n) funkcja Private VLAN,
 - o) możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
 - p) 5000 wpisów dla list kontroli dostępu (Security ACE),
 - q) funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www);

- 13) technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
- a) Trust Anchor Module – odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny,
 - b) Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego,
 - c) Image signing – obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności;
- 14) mechanizmy związane z zapewnieniem jakości usług w sieci:
- a) implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
 - b) implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
 - c) możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
 - d) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
 - e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 kbps (policing, rate limiting),
 - f) kontrola sztormów dla ruchu broadcast/multicast/unicast,
 - g) Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
- 15) obsługa protokołów routingu:
- a) routing statyczny dla IPv4 i IPv6,
 - b) routing dynamiczny – RIP, OSPF,
 - c) policy-based routing (PBR),
 - d) obsługa protokołu redundancji bramy (VRRP);
- 16) 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;
- 17) przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.);
- 18) zarządzanie:
- a) port konsoli,
 - b) dedykowany port Ethernet do zarządzania out-of-band,
 - c) 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,
 - d) obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, syslog – z wykorzystaniem protokołów IPv4 i IPv6,

- e) możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
 - f) przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
 - g) przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
 - h) port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- 19) możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU;
- 20) wsparcie dla protokołu LISP zgodnie z RFC 6830;
- 21) obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN);
- 22) obsługa zaawansowanych protokołów routingu:
- a) IS-IS i BGP dla IPv4 i IPv6,
 - b) EIGRP (rfc7868),
 - c) Routing multicastów – PIM-SM, PIM-SSM,
 - d) Multicast Source Discovery Protocol (MSDP),
 - e) VRF-Lite;
- 23) możliwość enkapsulacji ruchu w pakiety VXLAN;
- 24) możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym – NetFlow – obsługa 64.000 strumieni;
- 25) możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;
- 26) możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;
- 27) 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);
- 28) funkcjonalność bramy dla usług mDNS;
- 29) wbudowany analizator pakietów;
- 30) funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC;
- 31) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256);
- 32) wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol);
- 33) wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging);
- 34) przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7);
- 35) możliwość eksportu dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).

8.5.5 Przełączniki dostępne Typ 2

- 1) rodzaj urządzenia:
 - a) Przełącznik Gigabit Ethernet wyposażony w 24/48 portów 10/100/1000BaseT,

- b) porty uplink muszą umożliwiać obsadzenie modułami Gigabit Ethernet SFP (co najmniej 1000Base-T, 1000Base-SX, 1000Base-LX/LH) lub 10Gigabit Ethernet (co najmniej 10GBase-SR, 10GBase-LR,) zależnie od potrzeb Zamawiającego,
 - c) w razie potrzeby można zastosować przełącznik zapewniający PoE+;
- 2) wyposażenie:
- a) slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
 - 1G SFP,
 - 10G SFP+,
 - b) porty SFP/SFP+/QSFP możliwe do obsadzenia wkładkami zależnie od potrzeb:
 - porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,
 - porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax;
- 3) możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
- a) przepustowość w ramach stosu – 80Gb/s lub 160Gb/s,
 - b) 8 urządzeń w stosie,
 - c) zarządzanie poprzez jeden adres IP,
 - d) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
 - e) możliwość współdzielenia mocy zasilaczy (grupy do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (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);
- 4) zasilanie i chłodzenie:
- a) zasilacz prądem naprzemiennym 230V, możliwość instalacji zasilacza redundantnego,
 - b) redundantne i wymienne moduły wentylatorów,
 - c) przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności);
- 5) parametry wydajnościowe:
- a) szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
 - b) bufor pakietów – co najmniej 6MB,
 - c) pamięć DRAM – co najmniej 2GB,
 - d) pamięć flash – co najmniej 4GB,
 - e) obsługa:
 - 4.000 identyfikatorów sieci VLAN,
 - 16.000 adresów MAC,
 - 8.000 tras IPv4,
 - 1.500 tras IPv6;
- 6) obsługa protokołu NTP;
- 7) obsługa IGMPv1/2 i MLDv1/2 Snooping;

- 8) przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a) IEEE 802.1w Rapid Spanning Tree,
 - b) Per-VLAN Rapid Spanning Tree (PVRST+),
 - c) IEEE 802.1s Multi-Instance Spanning Tree,
 - d) Obsługa 128 instancji protokołu STP;
- 9) obsługa protokołu LLDP i LLDP-MED;
- 10) obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego;
- 11) możliwość uruchomienia funkcji serwera DHCP;
- 12) mechanizmy związane z bezpieczeństwem sieci:
 - a) wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
 - b) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
 - c) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
 - d) obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
 - e) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
 - f) możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
 - g) możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
 - h) obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
 - i) zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
 - j) możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
 - k) obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
 - l) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
 - m) wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
 - n) funkcja Private VLAN;
- 13) technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
 - a) Trust Anchor Module – odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny,

- b) Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmienny sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego,
 - c) Image signing – obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności;
- 14) mechanizmy związane z zapewnieniem jakości usług w sieci:
- a) implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
 - b) implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
 - c) możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
 - d) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
 - e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 kbps (policing, rate limiting),
 - f) kontrola sztormów dla ruchu broadcast/multicast/unicast,
 - g) możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
- 15) obsługa protokołów routingu:
- a) routing statyczny dla IPv4 i IPv6,
 - b) routing dynamiczny – RIP, OSPF,
 - c) policy-based routing (PBR),
 - d) obsługa protokołu redundancji bramy (VRRP);
- 16) 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;
- 17) przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.);
- 18) zarządzanie:
- a) port konsoli,
 - b) dedykowany port Ethernet do zarządzania out-of-band,
 - c) 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,
 - d) obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
 - e) możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
 - f) przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
 - g) przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,

- h) port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- 19) możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU;
- 20) wsparcie dla protokołu LISP zgodnie z RFC 6830;
- 21) obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN);
- 22) obsługa zaawansowanych protokołów routingu:
 - a) IS-IS dla IPv4 i IPv6,
 - b) EIGRP (rfc7868),
 - c) routing multicastów – PIM-SM, PIM-SSM,
 - d) Multicast Source Discovery Protocol (MSDP),
 - e) VRF-Lite;
- 23) możliwość enkapsulacji ruchu w pakiety VXLAN;
- 24) możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym – NetFlow – obsługa 16.000 / 32.000 strumieni;
- 25) możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;
- 26) możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;
- 27) 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 (RSPAN).

8.5.6 Przełączniki agregujące Typ 1

- 1) przełącznik z portami typu SFP/SFP+/SFP28/QSFP/QSFP28 (typ i liczba portów w zależności od potrzeb Zamawiającego);
- 2) slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
 - a) 25G/10G SFP28,
 - b) 1G SFP,
 - c) 10G SFP+,
 - d) 40G QSFP;
- 3) porty SFP/SFP+/SFP28/QSFP/QSFP28 możliwe do obsadzenia wkładkami zależnie od potrzeb np.:
 - a) porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
 - b) porty SFP28 – wkładki 25/10GBASE – w tym SFP-25G-SR-S, SFP-25G-SL, SFP-10/25G-CSR-S, SFP-10/25G-LR-S, FP-10/25G-LR-I, kable DAC i AOC,
 - c) porty QSFP – wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, twinax;
- 4) zasilanie i chłodzenie:
 - a) redundantne i wymienne moduły wentylatorów,
 - b) możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap);
- 5) parametry wydajnościowe:

- a) szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
- b) bufor pakietów – co najmniej 32 MB,
- c) pamięć DRAM – co najmniej 16 GB,
- d) pamięć flash – co najmniej 16 GB
- e) obsługa:
 - 4.000 identyfikatorów sieci VLAN,
 - co najmniej 64.000 adresów MAC,
 - co najmniej 64.000 tras IPv4,
 - co najmniej 32.000 tras IPv6;
- 6) obsługa protokołu NTP;
- 7) obsługa IGMPv1/2/3 i MLDv1/2 Snooping;
- 8) przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a) IEEE 802.1w Rapid Spanning Tree,
 - b) Per-VLAN Rapid Spanning Tree (PVRST+),
 - c) IEEE 802.1s Multi-Instance Spanning Tree,
 - d) obsługa 128 instancji protokołu STP;
- 9) obsługa protokołu 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) możliwość uruchomienia funkcji serwera DHCP;
- 13) mechanizmy związane z bezpieczeństwem sieci:
 - a) wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
 - b) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
 - c) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
 - d) obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
 - e) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
 - f) możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
 - g) możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
 - h) możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
 - i) 18.000 wpisów dla list kontroli dostępu (Security ACE),
 - j) funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www),
 - k) obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
 - l) zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych

- komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
- m) możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+;
 - n) obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
 - o) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch i switch-host) kluczami o długości 128-bitów (gcm-aes-128);
 - p) wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing);
 - q) funkcja Private VLAN;
- 14) technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
- a) Trust Anchor Module – odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny;
 - b) Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmienny sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego;
 - c) Image signing – obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności;
- 15) mechanizmy związane z zapewnieniem jakości usług w sieci:
- a) implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi;
 - b) implementacja algorytmu Shaped Round Robin dla obsługi kolejek;
 - c) możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority);
 - d) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP;
 - e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 kbps (policing, rate limiting);
 - f) kontrola sztormów dla ruchu broadcast/multicast/unicast;
 - g) 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:
- a) routing statyczny dla IPv4 i IPv6;
 - b) routing dynamiczny – RIP, OSPF;
 - c) policy-based routing (PBR);
 - d) 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:
- a) port konsoli,
 - b) dedykowany port Ethernet do zarządzania out-of-band,
 - c) 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,
 - d) obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
 - e) możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
 - f) przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
 - g) przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
 - h) port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- 20) możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU;
- 21) możliwość połączenia dwóch przełączników w stos (z wykorzystaniem standardowych modułów optycznych/twinax) celem stworzenia pojedynczego logicznego przełącznika z zapewnieniem następujących funkcjonalności:
- a) zarządzanie poprzez jeden adres IP,
 - b) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
 - c) możliwość aktualizacji oprogramowania w trakcie pracy stosu (ISSU – In Service Software Upgrade);
- 22) wsparcie dla protokołu LISP zgodnie z RFC 6830;
- 23) obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN);
- 24) obsługa zaawansowanych protokołów routingu:
- a) IS-IS i BGP dla IPv4 i IPv6,
 - b) EIGRP (rfc7868),
 - c) routing multicastów – PIM-SM, PIM-SSM,
 - d) Multicast Source Discovery Protocol (MSDP),
 - e) VRF-Lite;
- 25) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256);
- 26) możliwość enkapsulacji ruchu w pakiety VXLAN;
- 27) wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol);
- 28) wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging);
- 29) możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym – NetFlow – obsługa 128.000 strumieni;
- 30) możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;

- 31) możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;
- 32) funkcjonalność bramy dla usług mDNS;
- 33) wbudowany analizator pakietów;
- 34) 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);
- 35) przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7);
- 36) możliwość eksportu dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).

8.5.7 Przełączniki agregujące Typ 2

- 1) przełącznik z portami typu RJ-45/SFP/SFP+/SFP28/QSFP (typ i liczba portów w zależności od potrzeb Zamawiającego);
- 2) slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
 - a) 25G/10G SFP28,
 - b) 1G SFP,
 - c) 10G SFP+,
 - d) 40G QSFP;
- 3) porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia wkładkami zależnie od potrzeb np.:
 - a) porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,
 - b) porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
 - c) porty SFP28 – wkładki 25/10GBASE – w tym SFP-25G-SR-S, SFP-25G-SL, SFP-10/25G-CSR-S, SFP-10/25G-LR-S, FP-10/25G-LR-I, kable DAC i AOC,
 - d) porty QSFP – wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, adapter 40G QSFP->10G SFP+;
- 4) zasilanie i chłodzenie:
 - a) redundantne i wymienne moduły wentylatorów,
 - b) zasilacz prądem naprzemiennym 230V, możliwość instalacji zasilacza redundantnego,
 - c) przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności);
- 5) parametry wydajnościowe:
 - a) szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
 - b) bufor pakietów – co najmniej 16 MB,
 - c) pamięć DRAM – co najmniej 8 GB,
 - d) pamięć flash – co najmniej 16 GB,
 - e) obsługa:
 - 4.000 identyfikatorów sieci VLAN,

- co najmniej 32.000 adresów MAC,
 - co najmniej 24.000 tras IPv4,
 - co najmniej 16.000 tras IPv6;
- 6) obsługa protokołu NTP;
 - 7) obsługa IGMPv1/2/3 i MLDv1/2 Snooping;
 - 8) przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
 - a) IEEE 802.1w Rapid Spanning Tree,
 - b) Per-VLAN Rapid Spanning Tree (PVRST+),
 - c) IEEE 802.1s Multi-Instance Spanning Tree,
 - d) obsługa 128 instancji protokołu STP;
 - 9) obsługa protokołu LLDP i LLDP-MED.;
 - 10) funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC;
 - 11) obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego;
 - 12) możliwość uruchomienia funkcji serwera DHCP;
 - 13) mechanizmy związane z bezpieczeństwem sieci:
 - a) wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
 - b) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
 - c) autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
 - d) obsługa funkcji Guest VLAN umożliwiającą uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
 - e) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
 - f) możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
 - g) możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
 - h) możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
 - i) 5.000 wpisów dla list kontroli dostępu (Security ACE),
 - j) funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
 - k) obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
 - l) zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
 - m) możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
 - n) obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),

- o) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
 - p) wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
 - q) funkcja Private VLAN;
- 14) technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
- a) Trust Anchor Module – odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny,
 - b) Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmienny sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego,
 - c) Image signing – obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności;
- 15) mechanizmy związane z zapewnieniem jakości usług w sieci:
- a) implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
 - b) implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
 - c) możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
 - d) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
 - e) możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 kbps (policing, rate limiting),
 - f) kontrola sztormów dla ruchu broadcast/multicast/unicast,
 - g) 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:
- a) routing statyczny dla IPv4 i IPv6,
 - b) routing dynamiczny – RIP, OSPF,
 - c) Policy-based routing (PBR),
 - d) 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:
- a) port konsoli,
 - b) dedykowany port Ethernet do zarządzania out-of-band,

- c) 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,
 - d) obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
 - e) możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
 - f) przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
 - g) przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
 - h) port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
- 20) możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU;
- 21) możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
- a) zarządzanie poprzez jeden adres IP,
 - b) możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
 - c) możliwość współdzielenia mocy zasilaczy (grupy do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (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),
 - d) przepustowość w ramach stosu – 480Gb/s,
 - e) 8 urządzeń w stosie;
- 22) wsparcie dla protokołu LISP zgodnie z RFC 6830;
- 23) obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN);
- 24) obsługa zaawansowanych protokołów routingu:
- a) IS-IS i BGP dla IPv4 i IPv6,
 - b) EIGRP (rfc7868),
 - c) routing multicastów – PIM-SM, PIM-SSM,
 - d) Multicast Source Discovery Protocol (MSDP),
 - e) VRF-Lite;
- 25) możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256);
- 26) możliwość enkapsulacji ruchu w pakiety VXLAN;
- 27) wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol);
- 28) wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging);
- 29) możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym – NetFlow – obsługa 64.000 strumieni;
- 30) możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie;
- 31) możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;

- 32) funkcjonalność bramy dla usług mDNS;
- 33) wbudowany analizator pakietów;
- 34) 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);
- 35) przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7);
- 36) możliwość eksportu dodatkowych pól w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).

8.6 Urządzenia do obsługi ruchu CCTV

Przyjętym standardem dla aktywnych urządzeń sieciowych dla CCTV w Akademickiej Sieci Komputerowej WAT są urządzenia Zyxel.

9 WYMAGANIA W ZAKRESIE OKABLOWANIA SYSTEMÓW OCHRONY TECHNICZNEJ

Systemy ochrony technicznej:

- 1) CCTV;
- 2) I&HAS;
- 3) SKD;
- 4) depozytory;
- 5) SSP.

Urządzenia do transmisji sygnałów powinny mieć parametry zapewniające pracę w każdych warunkach pogodowych i środowiskowych. Tory transmisji sygnałów powinny zapewniać odporność na celowe lub przypadkowe uszkodzenie łącza oraz zabezpieczenie przed umyślnym przechwyceniem informacji transmitowanej tym łączem. Ponadto okablowanie tych urządzeń powinno być tak wykonane, aby wykluczyć możliwość wpięcia się w system osób nieupoważnionych lub przypadkowe przecięcie czy uszkodzenie przewodów.

Systemy transmisji sygnałów i komunikatów kierowanych do oddalonych centrów monitorowania powinny:

- 1) posiadać dwa tory transmisji sygnałów do oddalonego centrum monitorowania;
- 2) zapewniać transmisję i monitorowanie sygnałów potwierdzających sprawność monitorowanych systemów alarmowych i wykorzystywanych torów transmisji w okresach nie większych niż 180 s;
- 3) posiadać czas transmisji sygnału alarmowego nie dłuższy niż 20 s;
- 4) wskazywać szczegółowo występujące alarmy i komunikaty w stosunku do pojedynczych pomieszczeń podlegających ochronie w obiekcie;
- 5) wykrywać i przekazywać następujące sygnały z monitorowanego systemu:
 - a) włamania,
 - b) napadu,
 - c) sabotażu,
 - d) usterki technicznej,
 - e) awarii zasilania,
 - f) innych sygnałów wynikających z funkcjonalności systemu;

- 6) wykrywać próby manipulacji przy torach transmisji, ich modyfikacji lub próby zamiany urządzeń;
- 7) mieć dostępność systemu transmisji w każdym okresie 12 miesięcy nie mniejszą niż 99,5% miesięcznie;
- 8) posiadać środki chroniące przed nieautoryzowanym odczytem i modyfikacją transmitowanej informacji;
- 9) posiadać zabezpieczenie przed włamaniem, sabotażem i podmianą urządzenia nadawcze oraz inne urządzenia ważne z punktu widzenia transmisji sygnałów i komunikatów;
- 10) posiadać zabezpieczenie przed nieautoryzowaną modyfikacją informacji;
- 11) precyzować miejsca wystąpienia alarmu z dokładnością do budynku;
- 12) posiadać zabezpieczenie przed zastąpieniem urządzeń nadawczych przez dodanie adresu lub identyfikatora do każdej transmisji oraz szyfrowanie tego identyfikatora lub adresu przez dodanie unikalnego kodu dla każdego urządzenia albo w inny sposób.

W przypadku funkcjonowania w obiekcie wojskowym agregatów prądotwórczych uruchamiających się samoczynnie w czasie do 30 minut przy awarii zasilania podstawowego i gwarantujących bezprzerwową 36-godzinną pracę jako źródło rezerwowe należy stosować również akumulatorowe źródła zasilania rezerwowego zapewniające podtrzymanie zasilania przez co najmniej 4 h.

Nie należy uziemiać ani zerować kamer telewizyjnych zasilanych napięciem wyższym niż 24 V. W takim przypadku uziemione powinny być tylko obudowy tych kamer. Jeżeli zachodzi potrzeba uziemienia całego telewizyjnego systemu nadzoru, należy tego dokonać tylko w jednym punkcie instalacji, w centralnej tablicy zasilającej.

Zasilacze stosowane w nowo budowanych telewizyjnych systemach nadzoru powinny sygnalizować spadek napięcia rezerwowego źródła zasilania poniżej wymaganego poziomu, przy którym systemy alarmowe pracują poprawnie.

W rejonach o zwiększonym natężeniu wyładowań atmosferycznych urządzenia systemów nadzoru montowane w strefach ochrony zewnętrznej powinny być wyposażone w ochronę przeciwprzepięciową, montowaną na kablach sygnałowych i zasilających. Urządzenia ochrony przeciwprzepięciowej należy stosować na początku i końcu linii kablowej. Stosowane urządzenia ochrony przeciwprzepięciowej powinny być klasy B.

W rozległych telewizyjnych systemach nadzoru należy stosować urządzenia transmisji światłowodowej. **CCTV – kamery należy włączać do wyodrębnionej sieci LAN.** Preferowane zasilanie kamer POE.

W przypadku wątpliwości co do planowanego rozwiązania wymagana jest konsultacja z Sekcją Ochrony Obiektów Wojskowych, która podejmuje ostateczną decyzję.

9.1 Przewody miedziane

W przypadku przewodów miedzianych należy wybrać przewody wieloparowe i ekranowane, które są bardziej odporne na zakłócenia elektromagnetyczne pochodzące od innych urządzeń oraz instalacji. Przewody należy prowadzić w kanałach kablowych lub w listwach teletechnicznych (korytach, rurkach, szynach kablowych). Te najbardziej istotne należy chronić przed dostępem osób niepowołanych i chronić antysabotażowo. Podczas wykonywania instalacji alarmowych należy starać się, aby ich przewody były oddzielone od przewodów instalacji elektrycznej ze względu na możliwość generacji zakłóceń. Instalacje przewodowe należy wykonywać w technice konwencjonalnej (wieloprzewodowej) lub adresowalnej (magistralowej).

Ze względu na utrudnienia identyfikacji uszkodzonego lub będącego w stanie alarmu elementu (np. czujki) na jednym przewodzie nie dopuszcza się stosowania więcej niż jednego odbiornika.

Instalacje wykonane w technologii konwencjonalnej wykonywać w oparciu o przewód YTKSY 8x0.5 6x0.5 lub 4x0.5 w ekranie, który jest przeznaczony do instalacji alarmowych.

Technika adresowa (magistralowa) – wykorzystuje technologię magistrali danych. Każdy element na danej magistrali posiada własny adres i indywidualnie komunikuje się z centralą alarmową. Pozwala to nadzorować poszczególne urządzenia systemu alarmowego i w szeroki sposób wykorzystać możliwość identyfikacji elementów. Podstawową zaletą technologii magistralowej jest obniżenie kosztów ze względu na:

- 1) praktycznie brak zasadniczych ograniczeń projektowych i programowych;
- 2) możliwość podłączenia dużej ilości urządzeń na magistrali oraz mieszania różnych typów urządzeń;
- 3) skrócenie czasu projektowania przez ujednolicenie okablowania;
- 4) skrócenie czasu wykonania i wynikające z tego tytułu oszczędności w nakładach na materiały instalacyjne;
- 5) przejrzystość, elastyczność i prostota serwisu systemu;
- 6) niezawodność;
- 7) wysokie walory użytkowe i funkcjonalne;
- 8) odporność na zakłócenia i ujemny wpływ środowiska pracy;
- 9) niskie koszty konserwacji i serwisu.

Zasadniczym torem transmisji sygnałów i komunikatów w systemie alarmowym są łącza światłowodowe. Stosuje się je w obrębie pojedynczego kompleksu, w którym znajduje się Lokalne Centrum Nadzoru (LCN) / Oficer Dyżurny (OD WAT).

9.2 Przewody światłowodowe

Do transmisji sygnałów alarmowych pomiędzy budynkami lub do Lokalnego Centrum Nadzoru / Oficera Dyżurnego WAT należy wykorzystywać włókna światłowodowe jednomodowe.

Miejszem zbiorczym przewodów światłowodowych powinna być szafa RACK, zlokalizowana w danym budynku, ze złączem LC.

9.3 Zasilanie systemu

System nadzoru powinien być zasilany z minimum jednej fazy prądu przemiennego ~230 V +10% -15%, 50 Hz $\pm 2\%$ z wydzielonego i nadzorowanego punktu zasilania jako zasilanie podstawowe. System ten należy zasilać z wydzielonej i zabezpieczonej przed sabotażem tablicy rozdzielczej.

Zasilanie awaryjne powinno:

- 1) być zasilaniem integralnym, niewykorzystywanym przez inne urządzenia;
- 2) zapewniać normalną pracę systemu przez czas nie krótszy niż:
 - a) 12 h dla obiektów, w których pełnią ciągły dyżur służby serwisowe dysponujące częściami zamiennymi i mające do dyspozycji zastępcze źródła zasilania (np. agregaty prądotwórcze, dodatkowe akumulatory),
 - b) 36 h dla obiektów, w których istnieje ciągły dozór ludzki i dla których zagwarantowane są usługi serwisowe mające określony czas reakcji do 4 h,
 - c) 72 h dla pozostałych obiektów, w tym bez ciągłego dozoru ludzkiego;

- 3) zapewniać samoczynne przełączanie zasilania ze źródła podstawowego na rezerwowe i odwrotnie bez zakłócenia pracy systemu oraz sygnalizować w centrum nadzoru awarie zasilania podstawowego i powrót do niego.

10 WYMAGANIA W ZAKRESIE SYSTEMÓW SSP

W WAT tworzona jest sieć systemów sygnalizacji pożaru oparta na **Centrali Głównej POLON 4900s**, znajdującej się w pomieszczeniu Lokalnego Centrum Nadzoru i centralach w poszczególnych budynkach, zgodnie z **PN-EN 541:2011 Systemy sygnalizacji pożarowej (wszystkie części)**. Przekazanie sygnału z central z poszczególnych budynków do centrali głównej należy realizować w oparciu o medium transmisyjne – kabel światłowodowy. Zgodnie z wytycznymi producentów systemów ppoż. oraz obowiązującymi przepisami należy łączyć centrale **dwiema parami światłowodu**.

Przyjęte czasy dla central systemów sygnalizacji pożaru zlokalizowanych w obiektach WAT: T-1=60s, T-2=420s.

11 WYMAGANIA W ZAKRESIE INTEGRACJI SYSTEMÓW OCHRONY TECHNICZNEJ WAT

W celu integracji systemów w LCN należy spełnić warunki:

- 1) Centrala I&HAS *Galaxy* (należy przewidzieć wolny interfejs szeregowy lub *Ethernet* do integracji);
- 2) Depozytor kluczy: *SafeKey*;
- 3) Centrale pożarowe POLON 4900s wpięte w istniejące ringi światłowodowe;
- 4) SKD: w oparciu o centrale *Galaxy* lub *SKD Matrix*;
- 5) Kamery:
 - a) posiadające zaimplementowany protokół ONVIF (profil SI, T) i wymagana współpraca z systemem VMS *Avigilon*,
 - b) posiadające certyfikaty NDAA i TAA.

Ponadto:

- 1) do integracji każdego systemu należy dostarczyć lokalizację wszystkich jego elementów na podkładach DWG. Nazewnictwo elementów musi być zgodne z nazewnictwem udostępnianym przez protokół integracyjny;
- 2) należy zapewnić łączność sieciową między danym systemem, a serwerami aplikacyjnymi PSIM;
- 3) należy zapewnić łączność nowych systemów z istniejącym serwerem czasu.

12 DOBÓR LICZBY WŁÓKIEN ŚWIATŁOWODOWYCH

Dobierając kabel światłowodowy (min. 24 włókna) do połączeń budynkowych i międzybudynkowych, należy uwzględnić następującą wymaganą rezerwację włókien:

- | | |
|-------------------|---|
| 1) ASK sieć jawna | 4 |
| 2) ST MILNET-Z | 2 |
| 3) ST MILNET-I | 2 |

- 4) CCTV/Domofony 2
- 5) SKD 2
- 6) I&HAS 2
- 7) SSP 4

Razem daje to 18 włókien (9 par) zarezerwowanych na systemy WAT. Pozostałe włókna mogą zostać wykorzystane dowolnie po uzgodnieniu z DIN.

13 NORMY REFERENCYJNE

Normy dotyczące instalacji elektrycznych:

- 1) **PN-IEC 60364-5-512** Instalacje elektryczne w obiektach budowlanych
- 2) **PN-IEC 60364-1** Instalacje elektryczne niskiego napięcia
- 3) **PN-IEC 60364-4-411** Instalacje elektryczne niskiego napięcia. Ochrona dla zapewnienia bezpieczeństwa
- 4) **PN-IEC 60364-4-54** Instalacje elektryczne niskiego napięcia. Układy uziemiające i przewody ochronne

Normy dotyczące okablowania strukturalnego:

- 1) **ISO/IEC 11801 Ed.2.2: 2012 +A1/2** *Information Technology -- Generic cabling for customer premises*
- 2) **ISO/IEC 24764 Ed. 1.0 (2010-04)** *Information Technology -- Generic cabling for data centers*
- 3) **EN 50173-1:2011** *Information Technology -- Generic cabling systems -- Part 1 Generic requirements*
wraz z jej polskim odpowiednikiem:
PN-EN 50173-1:2011 Technika Informatyczna -- Systemy okablowania strukturalnego -- Część 1: Wymagania ogólne
- 4) **EN 50173-2:2007/A1:2010/AC:2011** *Information Technology -- Generic cabling systems -- Part 2 Office premises*
wraz z jej polskim odpowiednikiem:
PN-EN 50173-2:2008/A1:2011 Technika Informatyczna -- Systemy okablowania strukturalnego -- Część 2: Pomieszczenia biurowe
- 5) **EN 50173-5 : 2007/A2:2012** *Information Technology -- Generic cabling systems -- Part 5 Data centers*
wraz z jej polskim odpowiednikiem:
PN-EN 50173-5:2009/A1:2011E/A2:2013 Technika informatyczna -- Systemy okablowania strukturalnego -- Część 5: Centra danych
- 6) **N SEP-E-007:2017-09** Instalacje elektroenergetyczne i teletechniczne w budynkach. Dobór kabli i innych przewodów ze względu na ich reakcję na ogień

Normy dotyczące pomiarów sieci okablowania strukturalnego:

- 1) **PN-EN 50289-1-5:2008** Kable telekomunikacyjne -- Metody badań -- Część 1-5: Metody badań właściwości elektrycznych -- Pojemność.
- 2) **PN-EN 50289-1-6:2009** Kable telekomunikacyjne -- Metody badań -- Część 1-6: Metody badań właściwości elektrycznych -- Właściwości elektromagnetyczne.

- 3) **PN-EN 50289-3-9:2002** Kable telekomunikacyjne -- Metody badania -- Część 3-9: Metody badania właściwości mechanicznych -- Sprawdzanie odporności na przeginięcie.
- 4) **PN-EN 60068-2-14:2009** Badania środowiskowe -- Część 2-14: Próby -- Próba N: Zmiany temperatury.
- 5) **PN-EN 60352-3:2002** Połączenia nielutowane -- Część 3: Połączenia zakleszczane nielutowane dostępne -- Wymagania ogólne, metody badań i wskazówki praktyczne.

Normy referencyjne w zakresie instalacji i pomiarów:

- 1) **EN 50174-1:2018** *Information Technology -- Cabling installation -- Part 1: Installation specification and quality assurance*
wraz z jej polskim odpowiednikiem:
PN-EN 50174-1:2018-08 – wersja angielska Technika informatyczna -- Instalacja okablowania -- Część 1: Specyfikacja instalacji i zapewnienie jakości
- 2) **EN 50174-2:2018** *Information Technology -- Cabling installation -- Part 2: Installation planning and practices inside buildings*
wraz z jej polskim odpowiednikiem:
PN-EN 50174-2:2018-08 - wersja angielska Technika informatyczna -- Instalacja okablowania -- Część 2: Planowanie i wykonywanie instalacji wewnątrz budynków
- 3) **EN 50174-3:2013** *Information Technology -- Cabling system installation -- Part 3 – Industrial premises*
wraz z jej polskim odpowiednikiem:
PN-EN 50174-3:2014-02E Technika informatyczna -- Instalacja okablowania -- Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków
- 4) **EN 61935-1:2009** *Specification for the testing of balanced and coaxial information technology cabling -- Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards*
wraz z jej polskim odpowiednikiem:
PN-EN 61935-1:2010E Wymagania dotyczące sprawdzania symetrycznych i współosiowych kablowych linii telekomunikacyjnych -- Część 1: Okablowanie z symetrycznych kabli telekomunikacyjnych zgodne z serią norm **EN 50173**
- 5) **EN 50310:2016** *Telecommunications bonding networks for buildings and other structures*.
wraz z jej polskim odpowiednikiem:
PN-EN 50310:2016-09 Sieci połączeń wyrównawczych w budynkach i innych obiektach budowlanych z instalacjami telekomunikacyjnymi

Normy dotyczące systemów ochrony technicznej w zakresie wymagań eksploatacyjno-technicznych na podstawie Decyzji Nr 40/MON:

- 1) Instrukcja o ochronie obiektów wojskowych, sygn. **Sz. Gen. 1686/2017**
- 2) **PN-EN 50130-5:2012** Systemy alarmowe -- Część 5: Próby środowiskowe
- 3) **PN-EN 50131-1:2009** Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
- 4) **PN-EN 50131-1:2009/A1:2010** Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
- 5) **PN-EN 50132-5-3:2013-04** Systemy alarmowe. Systemy dozoru CCTV stosowane w zabezpieczeniach. Część 5-3 Transmisja wideo -- Analogowa i cyfrowa transmisja wideo

- 6) **PN-EN 60839-11-1:2014-1** Systemy alarmowe i Elektroniczne systemy zabezpieczeń -- Część 11-1 Elektroniczne systemy kontroli dostępu -- Wymagania dotyczące systemów i komponentów składowych
- 7) **PN-EN 62676-1-1:2014-06** Systemy dozoru CCTV stosowane w zabezpieczeniach Część 1-1: Wymagania systemowe -- Postanowienia ogólne
- 8) **PN-EN 62676-1-2:2014-06** Systemy dozoru CCTV stosowane w zabezpieczeniach Część 1-2: Wymagania systemowe -- Wymagania eksploatacyjne dotyczące transmisji wizji
- 9) **PN-EN 62676-2-1:2014-06** Systemy dozoru CCTV stosowane w zabezpieczeniach Część 2-1: Protokoły transmisji wizji -- Wymagania ogólne
- 10) **PN-EN 62676-2-2:2014-06** Systemy dozoru CCTV stosowane w zabezpieczeniach Część 2-2 Protokoły transmisji wizji -- Zastosowanie międzyoperacyjności IP oparte na usługach HTTP i REST
- 11) **PN-EN 62676-2-3:2014-06** Systemy dozoru CCTV stosowane w zabezpieczeniach Część 2-3 Protokoły transmisji wizji -- Zastosowanie międzyoperacyjności IP oparte na usługach Web
- 12) **PN-EN 62676-3:2015-11** Systemy dozoru wizyjnego stosowane w zabezpieczeniach Część 3: Analogowe i cyfrowe interfejsy wizyjne
- 13) **PN-EN 62676-4:2015-06** Systemy dozoru wizyjnego stosowane w zabezpieczeniach Część 4: Wytyczne zastosowania

Normy dotyczące systemów sygnalizacji pożaru:

- 1) **PN-EN 54-1:2011** Systemy sygnalizacji pożarowej -- wszystkie części

Normy dotyczące ochrony przeciwpożarowej:

- 2) **PN-EN 13501-2+A1:2010** Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków
- 3) **PN-EN 50575:2014** Klasyfikacja kabli pod względem pożarowym (Dyrektywa UE CPR)

Z uwagi na aktualizowanie norm, normami obowiązującymi są normy o aktualnej wersji.

14 SPIS RYSUNKÓW I TABEL

Spis rysunków

Rys. 1. Elementy funkcjonalne struktury hierarchicznej sieci	5
Rys. 2. Przywieszka identyfikacyjna kabla miedzianego	17
Rys. 3. Przywieszka identyfikacyjna kabla światłowodowego	18

Spis tabel

Tabela 1. Wymagane parametry kabla światłowodowego	7
Tabela 2. Wymagane parametry kabla światłowodowego preterminowanego złączami typu MPO	8
Tabela 3. Wymagane parametry kabla światłowodowego preterminowanego złączami typu LC	8

<i>Tabela 4. Wymagane parametry kaset światłowodowych typu MPO.....</i>	<i>10</i>
<i>Tabela 5. Wymagane parametry złącz światłowodowych</i>	<i>11</i>
<i>Tabela 6. Wymagane parametry kabla 4P</i>	<i>12</i>
<i>Tabela 7. Oznaczenia w przywieszce identyfikacyjnej kabla miedzianego</i>	<i>17</i>
<i>Tabela 8. Oznaczenia w przywieszce identyfikacyjnej kabla światłowodowego</i>	<i>18</i>

15 HISTORIA WERSJI

Nr wersji	Autor/Autorzy	Uwagi
1.00	płk Grzegorz Bobiński, mjr Piotr Jakubik, mjr Marcin Dąbkiewicz	Pierwsza wersja
1.01	płk Grzegorz Bobiński	Wersja po uzgodnieniach
2.00	ppłk Marcin Dąbkiewicz, Radosław Kłaskała, Andrzej Niburski	<ul style="list-style-type: none"> • aktualizacja wymagań dla części miedzianej (rozdz. 4.1 pkt. 7), światłowodowej (Tabela 1) oraz norm pomiarów sieci (rozdz. 4.5) • usunięto kable Kat. 6, klasę wydajności E, zmiana rodzajów łączy optycznych (rozdz. 4.2.1.1, w tym Tabela 4, rozdz. 4.2.2.3) • dodany wymóg inwentaryzacji, sposób wprowadzania kanalizacji do budynków oraz sposób oznaczania kabli (rozdz. 5) • dowiązanie do „Wykazu obowiązujących standardów sprzętu informatyki i oprogramowania do stosowania w Wojskowej Akademii Technicznej” (rozdz. 7) • aktualizacja typu złącza dla szaf zbiorczych (rozdz. 8.2) • aktualizacja norm w zakresie systemów ochrony technicznej (rozdz. 11)
3.00	płk Marcin Dąbkiewicz st. kpr. Weronika Nieradka Andrzej Niburski Leszek Derecki	<ul style="list-style-type: none"> • aktualizacja charakterystyki okablowania strukturalnego (rozdz. 3) • wydłużenie wymaganej gwarancji do 25 lat i uporządkowanie opisu, aktualizacja procedury odbiorowej (rozdz. 4) • dodano wymagania dotyczące kabli miedzianych (rozdz. 5.1), serwerowni budynkowych (rozdz. 6) • wskazano standardy w zakresie urządzeń aktywnych (rozdz. 8) oraz określono standard central dla systemu ppoż. (rozdz. 10) • dodano wymóg CCTV na wydzielonej sieci (rozdz. 9) • dodano wymagania w zakresie integracji systemów ochrony technicznej (rozdz. 11) • aktualizacja norm w zakresie systemów ochrony technicznej (rozdz. 13)