3.8.Szafy teletechniczne i akcesoria dodatkowe

Założono, że wszystkie urządzenia w węzłach szkieletowych WS oraz Punktach Dostępowych zainstalowane zostaną w zamykanych szafach teletechnicznych.

Zgodnie z uzgodnioną w roku 2009 koncepcją techniczną, opracowaną przez firmę EFICOM i uzgodnioną m.in. Przez Wydział Prawno-Organizacyjny, Centrum Zarządzania Siecią przewidziano w UM Czeladź.

W serwerowni Centrum Zarządzania istnieje już kompleks czterech szaf teletechnicznych, z czego jedna szafa teletechniczna zostaje przewidziana do inwestycji pn. „Rozwój społeczeństwa inwestycyjnego w Zagłębiu Dąbrowskim – Czeladź".

Wymagane jest zastosowanie zamykanych szaf 19", posiadających osłony boczne dla węzłów szkieletowych oraz punktów urządzeń abonenckich typu WiMAX. Rozwiązanie takie pozwoli zabezpieczyć urządzenia przed dostępem niepowołanych osób. Zapewnienie wymiany powietrza w szafie oraz efektywne chłodzenie zainstalowanego w niej sprzętu umożliwi zainstalowany wentylator sufitowy z termostatem. Poza tym szafa zostanie wyposażona w filtracyjną zaślepkę podłogową chroniącą przed zasysaniem kurzu do wnętrza szafy. W celu umożliwienia wyprowadzenia okablowania z dowolnej strony szafy zastosowany zostanie cokół wyposażony w ruchome stabilizatory chroniące szafę przed przewróceniem podczas wysuwania zainstalowanych wewnątrz urządzeń.

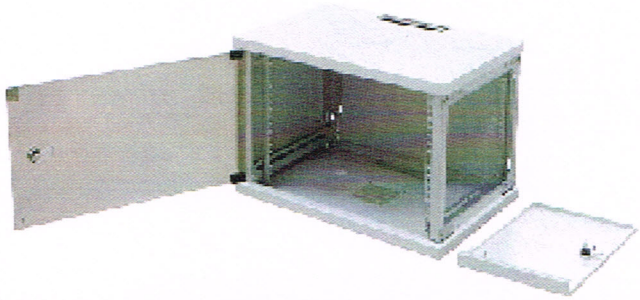
Szafa dystrybucyjna 42U przeznaczona jest do zastosowania w serwerowni. Wymagane jest aby model szafy dystrybucyjnej był zgodny z modelami szaf dystrybucyjnych znajdujących się z obecnej serwerowni.

W węzłach szkieletowych projektuje się zastosowanie szaf teletechnicznych o wysokości 18U, a w punktach dostępowych szaf teletechnicznych 12U.

- Konstrukcję szafki stanowi skręcany szkielet z drzwiami szklanymi lub blaszanymi, z odejmowanymi osłonami bocznymi i odkręcaną osłoną tylną.
- Standardowo szafka wyposażona jest w dwa kątowniki nośne o rozstawie 19" z płynną regulacją położenia, jedną zaślepkę wyłamywaną oraz przepust szczotkowy.
- Osłona tylna, osłony boczne oraz drzwi blaszane posiadają punkty uziemienia.
- Szafka mocowana jest bezpośrednio do ściany pomieszczenia bez konieczności stosowania

dodatkowych uchwytów - dobry dostęp do śrub mocujących od wewnętrznej strony szafki.

- Łatwa zamiana kierunku otwierania drzwi oraz orientacji otworów kablowych poprzez obrócenie szafki o 180°.
- Możliwość montażu dodatkowego wyposażenia wymienionego w rozdziale 3.8.1



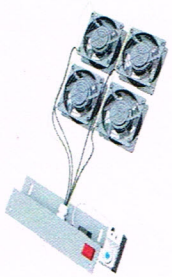
Rys. 3.8.a Przykładowy wygląd szafki teletechnicznej 12/18U

3.8.1. Dodatkowe elementy wyposażenia szaf teletechnicznych

Elementy te pozwalają zorganizować przebieg kabla wewnątrz szaf oraz jego doprowadzenie do szafy, a także zapewniają optymalne warunki pracy urządzeń aktywnych oraz ich zasilanie.

Panel wentylacyjny do szafy stojącej

Wentylatory przeznaczone są do montażu w szafach stojących serii MODBOX III. Zapewniają wymianę powietrza w szafie chroniąc zainstalowany sprzęt aktywny przed przegrzaniem. W skład wentylatora RAA-00177 wchodzą: cztery wentylatory, panel sterujący zakończony przewodem zasilającym o długości 2m z wtyczką, zestaw śrub montażowych. oraz termostat włączający obieg powietrza w przypadku przekroczenia zadanej temperatury wewnątrz szafy. W przedniej części panelu znajduje się wyłącznik zasilania oraz bezpiecznik.

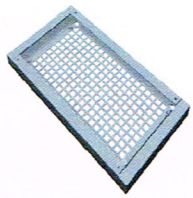


Parametry wentylatora:

- napięcie znamionowe: 220/230 V,
- częstotliwość: 50/60 Hz,

- moc znamionowa: 15/14 W,
- prąd znamionowy: 120/100 mA,
- prędkość obrotowa: 2600/2900 rpm,
- ciśnienie: 75/90 Pa
- wydajność: 162/192 m^3/h
- wymiary gabarytowe: 112 x 112 x 38 mm

Podłogowa zaślepka filtracyjna

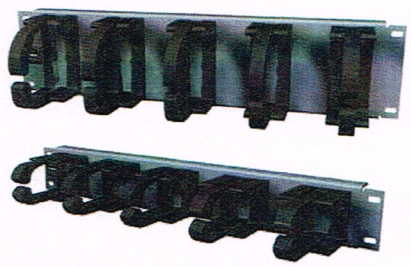


Filtracyjna zaślepka podłogowa szafy stojącej MODBOX IIII, chroni przed zasysaniem kurzu do wnętrza szafy. Nie wymaga specjalistycznych narzędzi montażowych (montaż przy pomocy śrub). Zaleca się stosowanie filtracyjnej zaślepki podłogowej w komplecie z wentylatorem do szaf MODBOX III.

Panel zasilający

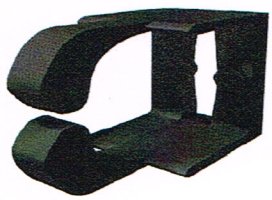
Panel 19-calowy, zasilający z bolcem uziemiającym (2P+Z) dedykowany do instalacji UPS, 7x230V/10A, wysokość 1U. Zaopatrzony jest w podświetlany wyłącznik odcinający zasilanie od wszystkich odbiorników. W skład zestawu wchodzą śruby montażowe.

Panele z wieszakami



Panel 19-calowy z wieszakami zapewnia estetyczny wygląd oraz uporządkowanie poziomych przebiegów kablowych w szafie. Ze względu na ilość kabli istnieje wersja 1U i 2U. Panel zapewnia łatwość częstej rekonfiguracji systemu z uwagi na grzebieniową konstrukcję. W skład zestawu wchodzą śruby montażowe.

Boczny wieszak kabla



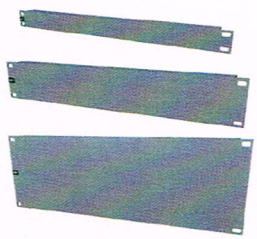
Porządkuje pionowe odcinki kabli krosowych w szafie dystrybucyjnej. Instalacja przy wykorzystaniu śrub montażowych paneli 19". Małe wymiary zewnętrzne.

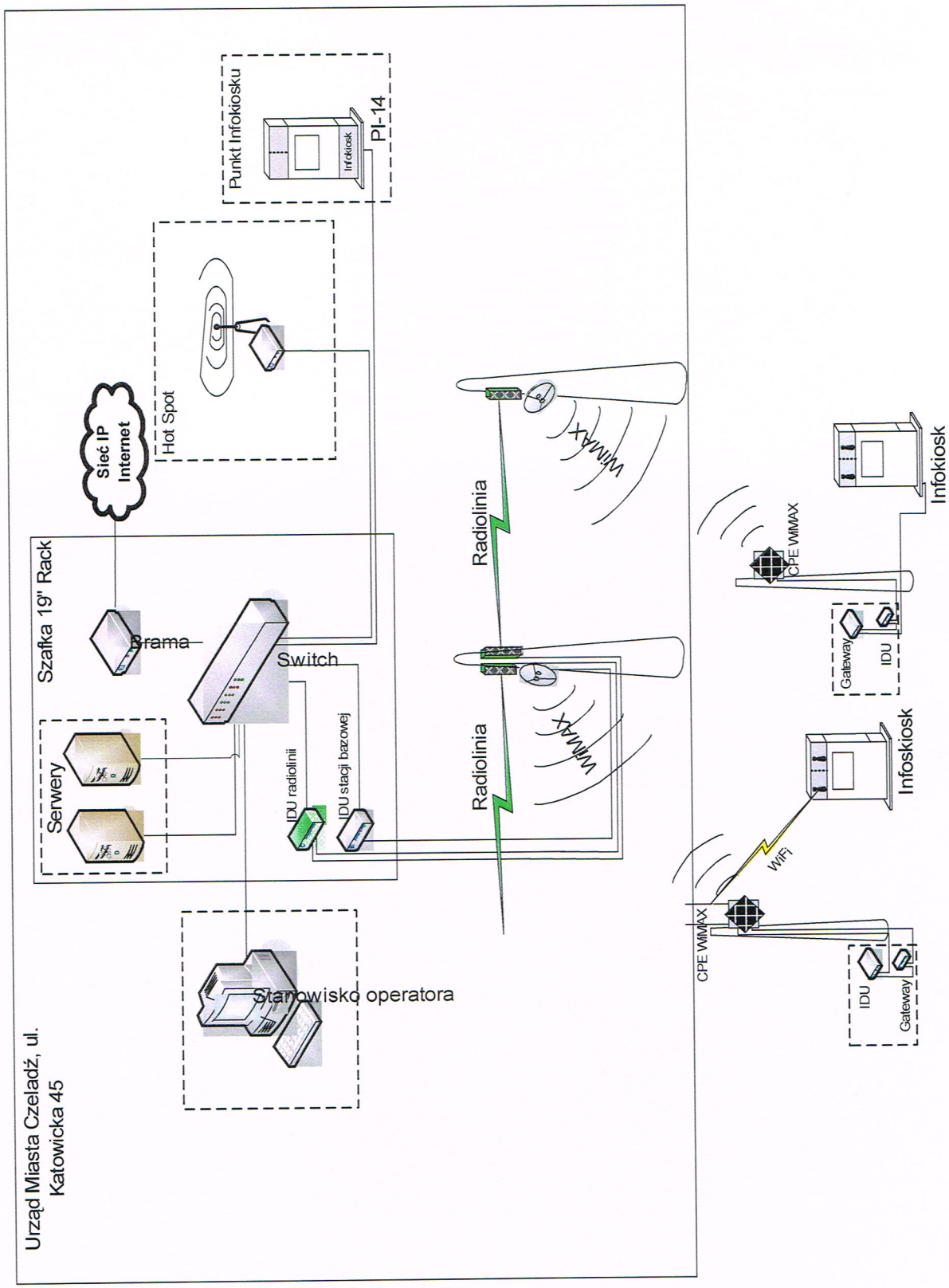
Pokrywa kablowa

Panel porządkujący przebiegi kablowe z pokrywą zasłaniającą kable krosowe, podnosząca estetykę punktu dystrybucyjnego. Mocowanie pokrywy za pomocą zatrzasków wykluczających konieczność stosowania specjalistycznych narzędzi. Standard 19". Łatwość częstej rekonfiguracji systemu z uwagi na grzebieniową konstrukcję. W skład zestawu wchodzą śruby montażowe. Przyjmuje do 50 kabli krosowych.

Panele osłonowe

Panel 19-calowy osłonowy przeznaczony do zaślepiania niewykorzystanej przestrzeni w szafie dystrybucyjnej lub na ramie montażowej w celu podwyższenia estetyki punktu rozdzielczego. Dostępny w rozmiarach 1U, 2U i 4U.





Rys 3.8.c Ideowy schemat połączeń elementów serwerowni

3.9.Zabezpieczenia systemu

Poniżej opisano zalecane zabezpieczenia poszczególnych elementów systemu, których zastosowanie pozwoli na monitorowanie poprawnego funkcjonowania oraz zmniejszy prawdopodobieństwo uszkodzenia poszczególnych elementów przez czynniki zewnętrzne.

3.9.1. Zalecane zabezpieczenia przełączników sieciowych

Poniższe punkty opisują zalecenia dotyczące mechanizmów bezpieczeństwa zalecanych przy konfiguracji przełączników sieciowych:

- Zdefiniowanie polityki bezpieczeństwa dla urządzeń typu switch dotyczącej następujących zagadnień:
  - system operacyjny,
  - hasła,
  - interfejs zarządzania,
  - usługi sieciowe,
  - zabezpieczenie interfejsów,
  - dostępność systemu,
  - sieci VLAN,
  - ustawienia protokołu STP,
  - uwierzytelnianie,
- Zabezpieczenie fizycznego dostępu do przełączników sieciowych
- Dostęp do interfejsu zarządzania przełącznikami poprzez inną podsieć VLAN, niż używaną w środowisku produkcyjnym,
- Zdefiniowanie czasu wygaśnięcia sesji użytkownika 'administrator',
- Konfiguracja urządzeń poprzez SSH i HTTPS (zdefiniowanie reguły blokującej dostęp do urządzeń poprzez Telnet i http),
- Uruchomienie tylko i wyłącznie potrzebnych usług sieciowych,
- Zdefiniowanie adresów MAC podłączonych do przełącznika urządzeń, zablokowanie możliwości podłączenia dodatkowych urządzeń do interfejsów przełącznika,

- Wyłączenie nieużywanych interfejsów przełącznika i przypisanie ich do sieci VLAN, która nie jest używana w środowisku produkcyjnym,
- Włączenie generowania logów i przesyłanie ich na dedykowany na potrzeby monitorowania serwer,

4. Infokioski

4.1.Wstęp

Zakłada się, że Infokioski będą dostępne dla społeczeństwa bezpośrednio w terenie Miasta Czeladzi. Infokiosk powinien być wykonany w wersji wolnostojącej, przystosowanej do eksploatacji w pomieszczeniach oraz na zewnątrz budynków. Powinien być wyposażony w monitor LCD, zabezpieczony szybą ze szkła hartowanego, klawiaturę o podwyższonej wytrzymałości, powinien mieć możliwość wbudowania w przyszłości głośników czy mikrofonu. Infokiosk powinien być zasilany z sieci o napięciu 230V, posiadać interfejs sieciowy LAN 10/100/1000. Infokioski powinny posiadać wbudowany system operacyjny, jak również oprogramowanie umożliwiające zdalne zarządzenie. Ilość Infokiosków oraz ich planowana lokalizacje są wskazane w tabeli nr 2. Dodatkowo szczegółowy lokalizacyjne oraz skompletowanie urządzeń dla planowanych lokalizacji Infokiosków regulują tzw. karty lokalizacyjne (załącznik).

Lokalizacja Infokiosków

Lp.	Infokioski	Lokalizacja
1	PI-01	ul. Szpitalna 9
2	PI-02	ul. Rynek-Bytomska
3	PI-03	ul. 1Maja 27
4	PI-04	Przystanek Lidl (Nowopogońska)
5	PI-05	ul. Dehnelów 10
6	PI-06	ul. 35-lecia 1
7	PI-07	ul. Wojkowicka
8	PI-08	ul. 11Listopada 8
9	PI-09	ul. Dehnelów 2
10	PI-10	ul. Katowicka-dehnelów
11	PI-11	ul. Francuska

12	PI-12	ul. Spacerowa 2
13	PI-13	ul. Sportowa 2
14	PI-14	ul. Katowicka 45
15	PI-15	ul. Szpitalna 2

4.2.Charakterystyka ogólna Infokiosków zewnętrznych.

Zadanie przewiduje montaż i uruchomienie 14 Infokiosków w wykonaniu zewnętrznym. Wszystkie Infokioski będą dostosowane do obsługi przez osoby niepełnosprawne (wózek inwalidzki). Szczegóły określają karty lokalizacyjne dla każdego Infokiosk osobno.

Infokiosk powinien być zaprojektowany z myślą o wykorzystaniu go w warunkach zewnątrz budynkowych. Obudowę terminala musi cechować wysoka estetyka wykonania i duża odporność na czynniki atmosferyczne.

Terminal ten służyć może jako element rozbudowanej sieci informacji jak również może spełniać rolę punktu publicznego dostępu do sieci Internet, Hot-Spot.

4.2.1. Opis techniczny Infokiosku zewnętrznego

Obudowa modułowa – trójczłonowa. Obudowa składająca się trzech niezależnych modułów. W przypadku uszkodzenia mechanicznego obudowy kiosku, możliwa jest wymiana każdego z modułów niezależnie od pozostałych. Elementy poszycia każdego modułu możliwe do wymiany w miejscu pracy urządzenia bez potrzeby przewożenia sprzętu do serwisu.

Obudowa składa się z modułów:

1. Dolnego – stanowiącego podstawę urządzenia,

2.Środkowego – będącego głównym elementem urządzenia,

W module środkowym przewidziano miejsce dla wszystkich urządzeń elektronicznych i elektrycznych – komputer, monitor dotykowy, urządzenia transmisji danych oraz ogrzewacz i wentylatory wraz z termostatem, integracja elementu bezpieczeństwa informatycznego Infokiosku. Ekran dotykowy osadzony w kasecie wykonanej z wysoko udarowego laminatu poliestrowego

lakierowanego na kolor z palety RAL określony przez Zamawiającego.

3. Górnego – element wieńczący z daszkiem osłonowym. W górnym module przewidziano miejsce na zabudowę komponentów (antena) systemu transmisji danych WiMAX lub Wi-Fi (możliwość doposażenia infokiosk w usługę dostępu bezprzewodowego w przyszłości).

Obudowa wykonana z materiału o niskiej tłumienności fal radiowych o częstotliwości od 2,4 do 5,8GHz.

Wewnętrzny szkielet aluminiowy wykonany z rur aluminiowych o przekroju kwadratowym 30x30x2 mm, malowany metodą proszkową.

Zewnętrzne elementy wykańczające boki terminala wykonane z dedykowanego profilu aluminiowego.

Elementy poszycia wykonane z blachy kwasoodpornej grubości przynajmniej 1,5mm – surowej lub malowanej proszkowo.

Poszycie Infokiosku wyizolowane w sposób zapewniający utrzymanie optymalnej temperatury we wnętrzu urządzenia.

W elementach poszycia zewnętrznego zamontowane kratki wentylacyjne z wysoko udarowego PCV zapewniające przewietrzanie wnętrza obudowy Infokiosku.

W module środkowym w przedniej części zabudowany monitor dotykowy

Drzwi rewizyjne zapewniające dostęp do komponentów elektronicznych w tylnej części obudowy (środkowy moduł) wykonane z blachy kwasoodpornej przynajmniej 1,5 mm z zawiasami trzpieniowymi spawanymi do ościeżnicy. Ościeżnica z zauszczelkowaną przylgą zapewniająca właściwą szczelność. Drzwi wyposażone z zasuwnicę z 4 punktami ryglowania blokowaną wkładką bębenkową wg normy DIN klasy bezpieczeństwa C.

Cała obudowa spełniająca normę szczelności IP 55.

Instalacja elektryczna:

Zasilanie 230 V, Moc infokiosk – pobór nie większy niż 600 W

Infokiosk wyposażony w wyłączniki różnicowo-prądowy oraz nadmiarowo-prądowy. W obudowie wydzielone dwa niezależne obwody elektryczne. Pierwszy zapewnia zasilanie komponentów

elektronicznych takich jak komputer, monitor z nakładką dotykową, komponenty radiowe itp., drugi do zasilenia układów grzewczych i wentylacyjnych oraz oświetlenia ogólnego Infokiosk.

Posadowienie:

Infokiosk posadowiony na prefabrykowanym postumencie betonowym o przekroju trapezu i wadze nie przekraczającej 200 kg, zbrojonego stalą z wypuszczonymi śrubami mocującymi fi 10 mm długości 100mm (ponad cokołem) i odpowiednimi kotwami.

Zamawiający oczekuje od Wykonawcy przedstawienia stosownego projektu wykonawczego fundamentu.

4.2.2. Opis techniczny Infokiosku zewnętrznego

Minimalne parametry techniczne osprzętu elektronicznego:

- **Jednostka centralna:**
  - Typ zainstalowanego procesora Intel Atom N270 1,6GHz lub równoważny
  - Pojemność zainstalowanego dysku min. 160 GB SATA II
  - Pojemność zainstalowanej pamięci min. 1024 MB
  - Ilość banków pamięci min 2 szt.
  - Ilość wolnych banków pamięci min. 1 szt.
  - Producent chipsetu zainstalowanej płyty głównej Intel lub równoważny
  - Typ zainstalowanego chipsetu 945GSE lub równoważny
  - Zintegrowana karta graficzna Tak
  - Zintegrowana karta dźwiękowa Tak
  - Zintegrowana karta sieciowa Tak
  - Typ zintegrowanej karty sieciowej min. 10/100/1000Mbit/s
  - Bezprzewodowa karta sieciowa Tak
  - Typ bezprzewodowej karty sieciowej IEEE 802.11b/g/n
  - Interfejsy

- min. 4 x USB 2.0
- min. 1 x RJ-45 (LAN)
- min 1 x wyjście liniowe
- min 1 x wyjście słuchawkowe
- min 1 x wejście na mikrofon
- min 1 x DVI

- System operacyjny Microsoft Windows XP Home PL. lub równoważny

- **Ekran LCD:**
- Przekątna min. 22"
- Typ matrycy TN lub równoważny
- Format obrazu: 16:10 lub 16:9 lub 4:3
- Nominalna rozdzielczość min 1680 x 1050
- Jasność min 300
- Kontrast min 50000
- Czas reakcji matrycy max.5
- Kąt widzenia w pionie min. 160
- Kąt widzenia w poziomie min. 170
- Ilość wyświetlanych kolorów 16,7 mln
- Gniazdo D-Sub min. 1 szt.
- Gniazdo DVI-D min. 1 szt.

- **Nakładka dotykowa pojemnościowa**:
- przejrzystości nie mniejszej niż 91%
- przynajmniej 1 kontroler USB
- rozdzielczość nakładki min. 16 x 16 tys. pkt.
- twardość powierzchni nie mniejsza niż 7H w skali Mohsa
- nie dopuszcza się stosowanie dodatkowych ramek z metalu lub tworzywa sztucznego

- **Parametry osprzętu elektrycznego**

Typ ogrzewania	Ogrzewanie z wentylatorem
Element grzejny	Wkład dużej mocy – min. 400W
Czujnik temperatury	Dla ochrony przed przegrzaniem na wypadek awarii wentylatora
Korpus grzewczy	Ciśnieniowy odlew aluminiowy (kula szklana obrabiana strumieniowo)
Zaciski	Zacisk trójbiegunowy 2,5mm²
Obudowa łącz	Tworzywo sztuczne UL94 V-0, czarne
Wentylator osiowy z łożyskami kulkowymi	Żywotność 50 000 h przy 25°C (77 °F)
Zaciski (wentylatora)	Zacisk dwubiegunowy 2,5mm² (L2/N2)
Zamocowanie	Klamra mocująca na szynach DIN 35 mm, EN 50022
Montaż	Poziomo
Temperatura pracy i składowania	-45 °C (-49 °F) do 70 °C (158 °F)
Rodzaj i klasa ochrony	IP 20 / II (z przewodem ochronnym) lub wyższa
Aprobacja	UL File No. E187294

Obudowa wentylatora i filtr wyjściowy	Materiał obudowy tworzywo sztuczne odporne na udary ASA UL94 H-B. Wysoka odporność na warunki atmosferyczne i promieniowanie nadfioletowe.
Wentylator osiowy	Z łożyskami kulkowymi, żywotność min. 50 000 h przy 25 °C (wilg. wzgl. 65 %). Ramka aluminiowa, wirnik z tworzywa sztucznego.
Podłączenie	2 lice, 100 mm, z zaciskami (bez potrzeby dokręcania) 2,5mm²
Wkład filtru	F5 według DIN EN 779, przeciętny stopień oczyszczania 98 %
Materiał filtrujący	Włókno sztuczne o budowie progresywnej, odporne na temperaturę do 100 °C, samo gaszące klasy F1
Temperatura pracy i składowania	-45 °C (-49 °F) do 70 °C (158 °F)
Rodzaj i klasa ochrony	IP 55/II (z przewodem ochronnym)

Oświetlenie zewnętrzne diodowe – listwa diodowa 500mm, 12V spełniająca normę szczelności IP65

Wymagania inne:

Certyfikat ISO 9001:2008 dla producenta oraz serwisu urządzenia

Certyfikat ISO 14001:2004 dla producenta oraz serwisu urządzenia

Deklaracja zgodności CE

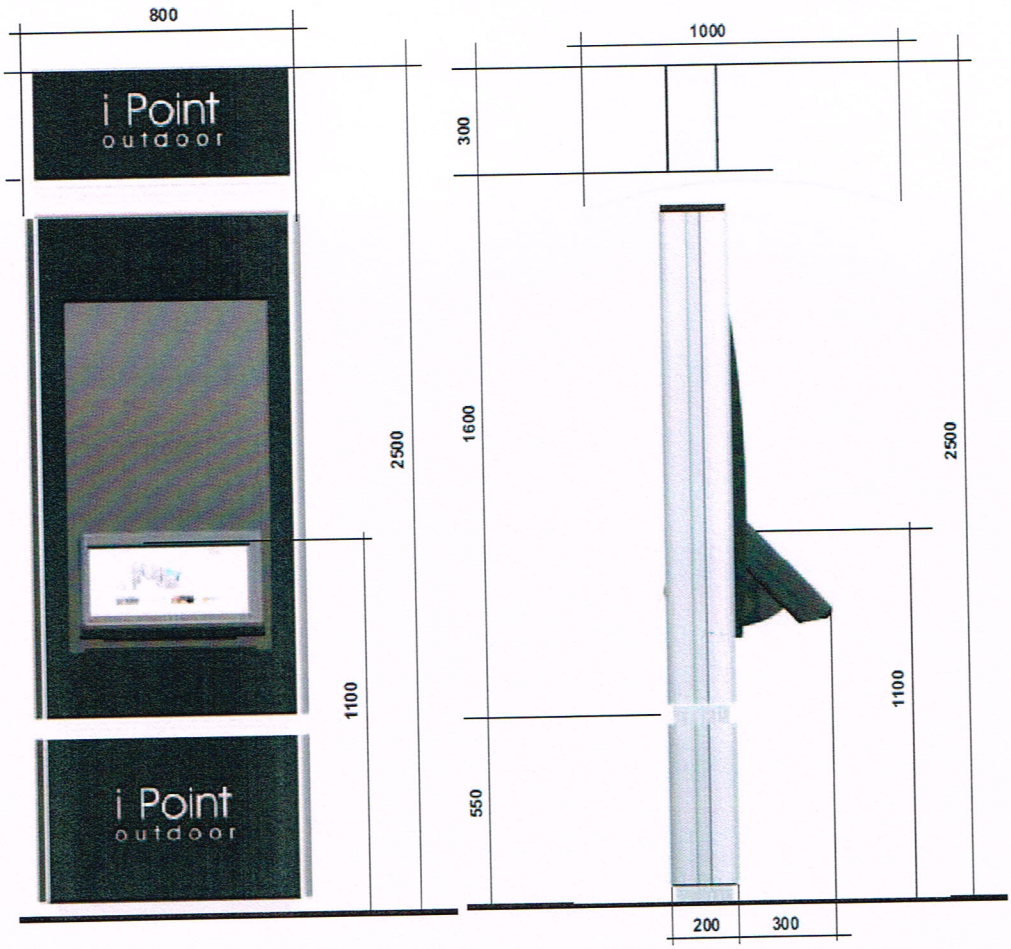
Wymiary maksymalne:

Wysokość 2500 mm

Szerokość 1000 mm

Głębokość 500 w wersji dla niepełnosprawnych (bez daszka osłonowego)

Przykładowa wizualizacja kiosku w wykonaniu zewnątrz budynkowym.



Rys. 4.2.3a Infokiosk zewnętrzny

4.2.3. Opis techniczny Infokiosku wewnętrznego

Infokiosk wolnostojący w wykonaniu wewnątrz budynkowym. Obudowa przystosowana do obsługi jej przez osoby niepełnosprawne poruszające się na wózku – wymagany podjazd do urządzenia przodem.

Obudowa trzyczłonowa – część dolna i górna zapewniająca możliwość umieszczenia podświetlanych elementów identyfikacji wizualnej, oraz środkowa z zabudowanym ekranem dotykowym umieszczonym pod kątem celem zapewnienia optymalnej pozycji za wszystkich jej użytkowników.

Dane techniczne

- Szkielet nośny wykonany z profili aluminiowych malowanych proszkowo.
- Elementy poszycia wykonane ze płyty aluminiowo-kompozytowej.
- Obudowa powinna umożliwiać bez narzędziową wymianę uszkodzonych elementów poszycia
- Dostęp serwisowy zabezpieczony dwoma niezależnymi zamkami, realizowany od tyłu obudowy poprzez otwarcie drzwi rewizyjnych.
- Obudowa górnego i dolnego modułu zapewniająca podświetlenie umieszczonych na niej elementów identyfikacji wizualnej.
- Podstawa stalowa malowana proszkowo, zapewniająca stabilność urządzenia, pozwalająca na zamocowanie obudowy infokiosku do posadzki.
- Otwór monitora zabezpieczony uszczelką silikonową o przekroju półokrągłym – nie dopuszcza się stosowania elementów z tworzywa sztucznego.
- Możliwość zabudowy szeregu elementów wyposażenia dodatkowego takich jak: kamera, mikrofon, klawiatura zewnętrzna itp.
- W przypadku uszkodzenia, obudowa powinna umożliwiać niezależną wymianę każdego z jej modułów na miejscu pracy urządzenia.

4.3. Opis techniczny Infokiosku wewnętrznego

Minimalne parametry techniczne osprzętu elektronicznego:

a) Jednostka centralna:

- Typ zainstalowanego procesora Intel Atom N270 1,6GHz lub równoważny
- Pojemność zainstalowanego dysku min. 160 GB SATA II

- Pojemność zainstalowanej pamięci min. 1024 MB
- Ilość banków pamięci min 2 szt.
- Ilość wolnych banków pamięci min. 1 szt.
- Producent chipsetu zainstalowanej płyty głównej Intel lub równoważny
- Typ zainstalowanego chipsetu 945GSE lub równoważny
- Zintegrowana karta graficzna Tak
- Zintegrowana karta dźwiękowa Tak
- Zintegrowana karta sieciowa Tak
- Typ zintegrowanej karty sieciowej min. 10/100/1000Mbit/s
- Bezprzewodowa karta sieciowa Tak
- Typ bezprzewodowej karty sieciowej IEEE 802.11b/g/n
- Interfejsy
  - min. 4 x USB 2.0
  - min. 1 x RJ-45 (LAN)
  - min 1 x wyjście liniowe
  - min 1 x wyjście słuchawkowe
  - min 1 x wejście na mikrofon
  - min 1 x DVI
- System operacyjny Microsoft Windows XP Home PL. lub równoważny

b) Ekran LCD:

- Przekątna min. 40"
- Typ matrycy TN, TFT lub równoważny
- Technologia podświetlania: CCFL lub równoważna
- Format obrazu: 16:10 lub 16:9 lub 4:3
- Nominalna rozdzielczość min 1600 x 900 pikseli
- Jasność min 300cd/m2
- Kontrast min 25000:1

- Czas reakcji matrycy max.5ms
- Kąt widzenia w pionie min. 170
- Kąt widzenia w poziomie min. 170
- Ilość wyświetlanych kolorów 16,7 mln

c) Nakładka dotykowa pojemnościowa:

- przejrzystości nie mniejszej niż 91%
- przynajmniej 1 kontroler USB
- rozdzielczość nakładki min. 16 x 16 tys. pkt.
- twardość powierzchni nie mniejsza niż 7H w skali Mohsa
- nie dopuszcza się stosowanie dodatkowych ramek z metalu lub tworzywa sztucznego

d) Zasilanie:

- Napięcie znamionowe, zmienne 230 V
- Maksymalna moc pobierana przez urządzenie – 100 W

Wymagania inne:

Certyfikat ISO 9001:2008 dla producenta oraz serwisu urządzenia

Certyfikat ISO 14001:2004 dla producenta oraz serwisu urządzenia

Deklaracja zgodności CE

Wymiary maksymalne:

szerokość – 600 mm (bez podstawy)

wysokość – 2000 mm

głębokość - 450 mm (bez podstawy)

Przykładowa wizualizacja infokiosku wewnętrznego

Rys.4.3a) Przykładowy model infokioksu wewnętrznego.

4.4. Wymagania funkcjonalne dla aplikacji kioskowej i systemu zarządzania siecią Infokiosków

1) Wymagania funkcjonalne dla aplikacji kioskowej – oprogramowania sterującego Infokioskiem:

- zabezpieczenie hasłem przed nieuprawnioną ingerencją w system operacyjny (możliwość zmiany domyślnej powłoki systemu),
- monitorowanie zajętości pamięci operacyjnej, wykonywanie restartu w przypadku przekroczenia limitu wolnej pamięci (tzw. Software Watch Dog),
- możliwość czyszczenia pliku stronicowania,
- możliwość automatycznego wyłączania/restartu (lub restartów) komputera o określonej godzinie,
- kontrola i ograniczanie dostępu do stron WWW (również blokada stron wprowadzanych po nr IP) - możliwość importowania z dowolnego pliku .txt listy domen dostępnych lub

zabronionych dla użytkownika,

- blokowanie dostępu do dysków,
- blokowanie krytycznych kombinacji klawiszy (CTRL+ ALT+ DEL, ALT+ TAB, CTRL+ AESC, ALT+ ESC, Windows) - możliwość dodawania własnych kombinacji do listy klawiszy, które mają być blokowane,
- obsługa czujników monitorujących bezpieczeństwo kiosku – czujniki wstrząsowe, otwarcia drzwi itp. z możliwością powiadomienia administratora, ochrony itp. za pośrednictwem np. maila lub modułu komunikacyjnego. Możliwość uruchomienia zapisu z wbudowanej kamery celem identyfikacji sprawcy ewentualnych zniszczeń,
- dostosowanie aplikacji do po obsługi przez osoby słabo widzące nie tylko poprzez funkcjonalność powiększania wyświetlania treści ale także poprzez zastosowanie funkcji monochromatycznego wyświetlania obrazu,
- obsługa modułu bluetooth pozwalająca na komunikację z telefonami komórkowymi w zakresie wysyłania z kiosku wybranego kontentu na telefon,
- blokowanie wyświetlania wyskakujących okien,
- możliwość określenia listy stron WWW, na których wyskakujące okna nie będą blokowane,
- możliwość wyświetlania w dedykowanym module aplikacji lokalnie zainstalowanych filmów, galerii zdjęć i dokumentów,
- edycja i wyświetlanie dowolnych ogłoszeń z opcją ich wydruku (możliwość edycji parametrów wydruku ogłoszeń – nagłówek, czcionka, marginesy),
- przeglądarka internetowa w trybie wielookienkowym (wybór aktywnego okna za pomocą zakładek),
- możliwość definiowania wyglądu przeglądarki (administrator musi mieć możliwość określania widoczności przycisków oraz ukrycia paska adresu i paska zakładek),
- funkcja powiększania przeglądanych stron www – możliwość zdefiniowania domyślnego powiększenia dla dowolnej strony www,
- definiowanie ustawień ograniczających dostęp do różnych rodzajów zasobów: filmy,

skrypty itp.

- wirtualna klawiatura z możliwością przemieszczania po ekranie,
- regulowany stopień przeźroczystości klawiatury w stanie podstawowym i podczas przemieszczania,
- możliwość określenia domyślnego położenia niezadokowanej klawiatury, zmiany rozmiaru i zdefiniowania trybu pracy (zadokowana lub niezadokowana),
- automatyczne wysuwanie klawiatury po wybraniu przez użytkownika pola tekstowego,
- wysyłanie poczty elektronicznej z dedykowanego modułu aplikacji (administrator musi mieć możliwość wyboru załączników, edycji tekstu dołączonego w stopce wiadomości, edycji formatu wiadomości - w tym tła),
- przeglądanie podanej przez użytkownika skrzynki pocztowej z dedykowanego modułu aplikacji (nie w przeglądarce internetowej) bez możliwości zapisu treści poczty i załączników oraz ich uruchamiania,
- definiowanie programów dostępnych do uruchomienia przez użytkownika kiosku (w tym możliwość zdefiniowania aplikacji, która może być uruchamiana podczas startu programu)
- możliwość samodzielnego tworzenia aplikacji z wielopoziomowym systemem nawigacji (możliwość tworzenia dowolnej liczby ekranów z przyciskami),
- możliwość edycji interfejsu użytkownika - określanie widoczności przycisków, napisy na przyciskach, edytowanie tytułu i podtytułu aplikacji, możliwość dodania własnego logo, wstawienia grafik,
- możliwość zdefiniowania czynności, które mają być wykonane po naciśnięciu przez użytkownika danego przycisku (aplikacja musi umożliwić m.in. wyświetlania dowolnej strony internetowej, uruchomienia modułu wysyłania poczty elektronicznej, uruchomienie modułu odczytu e-mail, przejście do kolejnego ekranu z przyciskami, wyświetlenie lokalnie zainstalowanego dokumentu .pdf, pliku .html, pliku video w formacie .wmv lub .avi, galerii zdjęć, uruchomienie dowolnej aplikacji),
- możliwość gromadzenia statystyk - raporty wysyłane na dowolny adres e-mail

z możliwością zdefiniowania zdarzeń rejestrowanych w raportach,

- wysyłanie powiadomień o pracy kiosku z możliwością zdefiniowania, jakie informacje mają być wysłane na wskazany adres e-mail (dla każdej informacji musi istnieć możliwość zdefiniowania odrębnego adresu e-mail),
- możliwość definiowania częstotliwości wysyłania informacji o pracy kiosku,
- licznik dotknięć - możliwość przedstawienia w formie graficznej i wysyłania na dowolny adres e-mail historii aktywności użytkowania danego kiosku,
- wyświetlanie dowolnej liczby wygaszaczy ekranu (możliwość zdefiniowania galerii zdjęć jako wygaszacza),
- wykonywanie zrzutów z kamery i/lub ekranu z opcją składowania tych obrazów na lokalnym dysku i/lub na dowolnym serwerze,
- obsługa czujnika ruchu (definiowanie zdarzeń, które mogą być wywoływane – w tym zamknięcie wygaszacza ekranu, uruchamiania dowolnego pliku dźwiękowego w formacie .wav, uruchamianie dowolnej aplikacji),
- wielojęzyczny interfejs użytkownika (możliwość samodzielnej edycji napisów i komunikatów w poszczególnych wersjach językowych),
- dostęp do ustawień i konfiguracji chroniony hasłem,
- możliwość eksportu i importu ustawień aplikacji,
- konfigurator w języku polskim

UWAGA: Zamawiający wymaga 5 lat gwarancji na oprogramowanie aplikacji kioskowej i modernizację wersji oprogramowania w ciągu tego okresu.

2) Wymagania funkcjonalne dla centralnego systemu zarządzania siecią Infokiosków

Minimalne wymagania funkcjonalne dla aplikacji zdalnego zarządzania Infokioskami

a) system musi umożliwiać zarządzanie kioskami przez Internet (kioski nie posiadają stałego adresu IP). Ze względów bezpieczeństwa zarządzanie kioskami powinno być realizowane przez aplikację systemu Windows - nie przez przeglądarkę WWW

b) Oprogramowanie powinno umożliwiać m.in.:

- sprawdzanie statusu (aktywności) kiosku,
- monitorowanie pracy kiosków,
- wydruk informacji o wykonanych przez kiosk czynnościach w określonym przedziale czasowym,
- zdalny restart lub wyłączenie kiosku,
- zmiany strony startowej przeglądarki,
- zmiany ustawień parametrów filtrowania (m. in. dostępnych protokołów, dostępnych i zabronionych fraz i domen),
- zmiany konfiguracji aplikacji zainstalowanej w kiosku - ustawień przeglądarki internetowej, poczty elektronicznej, wirtualnej klawiatury, blokowania wyskakujących okien, wysyłania powiadomień o pracy aplikacji, raportów, monitoringu, godzin restartów i wyłączeń kiosku,
- sprawdzanie informacji o systemie - zainstalowanym sprzęcie, dostępnej pamięci operacyjnej, miejscu na dyskach twardych, zainstalowanych kamerach i drukarkach, uruchomionych usługach itd.,
- zarządzanie plikami wygaszaczy (zdalne dodanie, usunięcie wygaszacza),
- pobranie historii aktywności użytkowania danego kiosku w określonym przedziale czasowym,
- wydruk statystyk użytkowania kiosku,
- ustawianie parametrów wykonywania zrzutów z kamery i ekranu,
- możliwość pobrania aktualnego zrzutu ekranu i z kamery z wybranego kiosku,
- konfigurację ekranu startowego (widoczność przycisków, edycja napisów, definiowanie czynności, która ma być wykonana po naciśnięciu przez użytkownika danego przycisku, dodawanie grafik),
- wysyłanie poleceń do jednego, kilku lub wszystkich kiosków jednocześnie,
- zarządzanie i monitorowanie pracy kiosków przez użytkowników z różnymi poziomami uprawnień - definiowanie grup urządzeń, zarządzanie nimi na różnych prawach,

4.5. Wymagania dla systemu zabezpieczenia systemów informatycznych Infokiosków i zapewnienie bezpieczeństwa pracy sieci Infokiosków i jej użytkowników.

Kluczowym elementem systemu zabezpieczeń sieci infokiosków będzie wielofunkcyjny system bezpieczeństwa klasy UTM składający się z następujących komponentów funkcjonalnych:

- Firewall klasy Stateful Inspection
- Antivirus
- System detekcji i prewencji włamań (IDP)
- VPN, zgodny z IPSec, PPTP i L2TP oraz SSL- VPN
- Antyspam
- Filtracja stron www
- Kontrola pasma (Traffic Management)

Każdy Infokiosk, niezależnie od przeznaczenia i sposobu montażu, zostanie wyposażony w gateway o funkcjonalności i minimalnych wymaganiach technicznych, przedstawionych poniżej (TYP A, razem 15 szt.). Gateway zostanie zintegrowany mechanicznie z obudową Infokiosk i programowo z jego jednostką centralną.

Dla węzła centralnego, do którego będzie się schodził ruch do i z Internetu dla Infokiosków, przewidziano montaż 1 szt. urządzenia klasy UTM (TYP B, razem 1 szt.) o parametrach pozwalających na stabilną i bezpieczną pracę sieci Infokiosków. Minimalne wymagania dla tego elementu bezpieczeństwa sieci Infokiosków podane są w dalszej części niniejszego dokumentu.

Element bezpieczeństwa UTM ma zapewnić następującą funkcjonalność (dot. TYP A i TYP B):

- Blokowanie prób nieupoważnionego dostępu zgodnie z ustaloną polityką bezpieczeństwa (kontrola i ograniczenie dostępu do sieci wewnętrznej).
- Inspekcja ruchu sieciowego na wielu poziomach (m.in. firewall prowadzi kontrolę na podstawie adresów IP, kierunku i stanu połączeń, protokołów i aplikacji, indywidualnych użytkowników).
- Tworzenie stref bezpieczeństwa i modelowanie charakterystyki ruchu między nimi.

- Szybkie powiadamianie administratorów w sytuacjach wyjątkowych (np. poprzez alarm na konsolę lub e-mail).
- Gromadzenie logów o zaistniałych zdarzeniach oraz zapewnienie możliwości tworzenia statystyk i raportów.
- Wykrywanie i blokowanie penetracji i ataków wykonywanych przez intruzów i robaki internetowe za pomocą wielu metod detekcji Wykrywanie ataków (D) DoS przez sygnatury i analizę ruchu sieciowego (przekroczenie wartości progowych).
- Funkcjonalność antywirusowa zaimplementowana w oparciu o sprzętowy akcelerator (ASIC) .
- Skanowanie antywirusowe protokołów HTTP, FTP, POP3, IMAP i SMTP
- Skanowanie AV zarówno na bazie sygnatur jak i heurystycznie
- Obsługa NAT dla VPN
- Moduł antyspamowy w obrębie protokołów SMTP, POP3 i IMAP bazujący na wielu czynnikach, takich jak:
    - sprawdzenie zdefiniowanych przez administratora adresów IP przez które przechodził mail,
    - sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
    - RBL, ORDBL
    - Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych
- Moduł filtracji stron WWW filtrujący na bazie:
    - białej i czarnej listy URL
    - W oparciu o zawarte w stronie słowa kluczowe
    - Javy, cookies i ActiveX
- Urządzenie musi wspierać różne poziomy i domeny uprawnień dla administratorów

Dostarczony sprzęt musi być objęty 5 letnią gwarancją. Dodatkowo wykonawca dostarczy w ramach zamówienia subskrypcję szczepionek (wszelkie aktualizacje), w zakresie Firewall klasy Stateful Inspection, Antywirus, System detekcji i prewencji włamań (IDP), VPN (zgodny z IP Sec, PPTP i L2TP oraz SSL- VPN), Antyspam, Filtracja stron WWW, Kontrola pasma (Traffic Management), na okres 5lat.

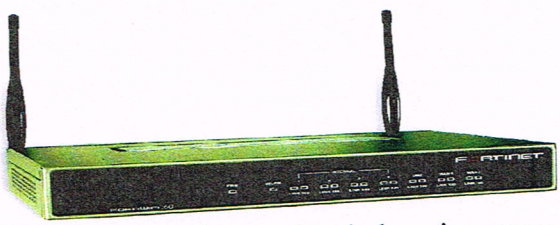
4.6. Minimalne wymagania techniczno – funkcjonalne dla elementu bezpieczeństwa informatycznego Infokiosku (TYP A).

Lp.	Parametr	Minimalne wymagania techniczno-funkcjonalne elementu bezpieczeństwa infokiosków
1	Architektura systemu ochrony	System ochrony musi być zbudowany przy użyciu minimalnej ilości elementów ruchomych, krytycznych dla jego działania. Dlatego, główne urządzenie ochronne [gateway] nie może posiadać twardego dysku, w zamian używać pamięci FLASH. Podstawowe funkcje systemu muszą być realizowane (akcelerowane) sprzętowo przy użyciu specjalizoanego układu ASIC. Jednocześnie, dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta, który udzieli odbiorcy licencji bez limitu chronionych użytkowników (licencja na urządzenie). Uwaga: Dziennik zdarzeń lub inne działania wymagające systemów dyskowych muszą być realizowane na zewnętrznych, dedykowanych do tego celu urządzeniach
2	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia
3	Ilość/rodzaj portów	Nie mniej niż 3 porty Ethernet 10/100 Base-T Nie mniej niż 2 porty WAN Ethernet 10/100 Base-T
4	Funkcjonalności podstawowe i uzupełniające	System ochrony musi obsługiwać w ramach jednego urządzenia wszystkie z poniższych funkcjonalności podstawowych: • kontrolę dostępu - zaporę ogniową klasy Stateful Inspection • ochronę przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM) • poufność danych - IPSec VPN oraz SSL VPN • ochronę przed atakami - Intrusion Prevention System [IPS/IDS] oraz funkcjonalności uzupełniających:

		• kontrolę treści – Web Filter [WF] • kontrolę zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP) • kontrolę pasma oraz ruchu [QoS i Traffic shaping] • kontrolę aplikacji (wsparcie dla co najmniej tysiąca aplikacji w tym IM oraz P2P) • zapobieganie przed wyciekiem informacji poufnej DLP (Data Leak Preention)
5	Zasada działania (tryby)	Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: • jako router/NAT (3.warstwa ISO-OSI) lub • jako most /transparent bridge/. Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu • jako router bezprzewodowy pracujący w standardzie WiFi 802.11 b/g
6	Polityka bezpieczeństwa (firewall)	Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ)
7	Wykrywanie ataków	Wykrywanie i blokowanie technik i ataków stosowanych przez hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX). Ochronę sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP. 1. Nie mniej niż 3900 sygnatur ataków. 2. Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie 3. Możliwość wykrywania anomalii protokołów i ruchu
8	Translacja adresów	Statyczna i dynamiczna translacja adresów (NAT). Translacja NAPT
9	Zarządzanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającm: • Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej • Wersjonowanie polityk w taki sposób aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości • Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia

		• Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia • Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM) • Zapis i zdalne wykonywanie skryptów na urządzeniach
10	Raportowanie	System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem raportowania i korelacji logów umożliwiającym: • Zbieranie logów z urządzeń bezpieczeństwa • Generowanie raportów • Skanowanie podatności stacji w sieci • Zdalną kwarantannę dla modułu antywirusowego
11	Integracja systemu zarządzania	Zgodnie z zaleceniami normy PN-ISO/17799 zarówno moduł centralnego zarządzania jak i raportowania muszą być zrealizowane na osobnych urządzeniach sprzętowych. Jednocześnie administrator powinien mieć do dyspozycji jedną konsolę zarządzającą do kontroli obu podsystemów.
12	Serwis oraz aktualizacje	Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 5 lat. System powinien być objęty serwisem gwarancyjnym producenta przez okres 5 lat.
13	Wymiany maksymalne (HxWxL), waga	4 cm x 22 cm x 15 cm, waga nie więcej niż 1 kg (konieczność integracji mechanicznej z obudową infokiosku)
14	Maksymalny pobór mowy w trybie pracy	Nie więcej niż 30 W

Przykładowe urządzenie bezpieczeństwa dostępu do Internetu zaprezentowano na rysunku 4.6a



Rys. 4.6a Przykładowe rozwiązanie urządzenia bezpiecznego dostępu do Interntu

4.7. Minimalne wymagania techniczno – funkcjonalne dla elementu bezpieczeństwa informatycznego Infokiosku (TYP B).

Minimalne wymagania funkcjonalno-techniczne:

Kluczowym elementem systemu bezpieczeństwa sieci Infokiosków będzie wielofunkcyjny system bezpieczeństwa klasy UTM, obsługujący w ramach jednego urządzenia wszystkie z poniższych funkcjonalności:

1. Kontrolę dostępu - zaporę ogniową klasy Stateful Inspection,
2. Ochronę przed wirusami – antywirus (AV) (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, IM),
3. Poufność danych - IPSec VPN oraz SSL VPN
4. Ochronę przed atakami - Intrusion Prevention System (IPS/IDS)
5. Kontrolę treści – Web Filter (WF)
6. Kontrolę zawartości poczty – antyspam (AS) (dla protokołów SMTP, POP3, IMAP)
7. Kontrolę pasma oraz ruchu (QoS i Traffic shaping)
8. Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenia ochronne muszą pracować w oparciu o dedykowany system operacyjny czasu rzeczywistego. Nie dopuszcza się stosowania komercyjnych systemów operacyjnych, ogólnego przeznaczenia. Jednocześnie, wymaga się aby wszystkie funkcje ochronne oraz zastosowane technologie, w tym system operacyjny pochodziły od jednego producenta. Licencja musi być udzielana na urządzenie, bez limitu chronionych użytkowników
9. Urządzenie powinno dawać możliwość ustawienia jednego z dwóch trybów pracy: jako router/NAT (3.warstwa ISO-OSI) lub jako most (transparent bridge). Tryb przezroczysty umożliwia wdrożenie urządzenia bez modyfikacji topologii sieci niemal w dowolnym jej miejscu.
10. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły i usługi sieciowe, użytkowników aplikacji, domeny, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasmo gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
11. Musi istnieć możliwość wykrywania i blokowania technik i ataków stosowanych przez

hakerów (m.in. IP Spoofing, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów (m.in. Java/ActiveX), a także ochrona sieci VPN przed atakami Replay Attack oraz limitowanie maksymalnej liczby otwartych sesji z jednego adresu IP.

12. Urządzenie powinno umożliwić definiowanie w jednym urządzeniu bez dodatkowych licencji nie mniej niż 10 wirtualnych firewalli, gdzie każdy z nich posiada indywidualne tabele routingu, polityki bezpieczeństwa i dostęp administracyjny. Obsługa Policy Routingu powinna być realizowana w oparciu o typ protokołu, numeru portu, interfejsu, adresu IP źródłowego oraz docelowego.
13. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników. Rozwiązanie powinno umożliwiać budowę logowania Single Sign On w środowisku Active Directory bez dodatkowych opłat licencyjnych.
14. Producent powinien dysponować certyfikatami potwierdzającymi wysoką skuteczność systemów bezpieczeństwa.
15. Urządzenie bezpieczeństwa powinno ponadto spełniać poniższe wymagania:

- Nie mniej niż 6 portów Ethernet 10/100Base-T i nie mniej niż 2 porty Ethernet 10/100/1000Base-T.
- Nie mniej niż 3900 sygnatur ataków.
- Aktualizacja bazy sygnatur ma się odbywać ręcznie lub automatycznie.
- Możliwość wykrywania anomalii protokołów i ruchu.
- Obsługa nie mniej niż 400.000 jednoczesnych połączeń i 10.000 nowych połączeń na sekundę.
- Przepływność nie mniejsza niż 450Mbps dla ruchu nieszyfrowanego i 100Mbps dla VPN (3DES).
- Obsługa nie mniej niż 1000 jednoczesnych tuneli VPN.
- Statyczna i dynamiczna translacja adresów (NAT).
- Tworzenie połączeń w topologii Site-to-site oraz Client-to-site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Konfiguracja w oparciu o politykę bezpieczeństwa (policy based VPN) i tabele routingu (interface based VPN).

- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth.
- Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
- Możliwość połączenia dwóch identycznych urządzeń w klaster.

16. Obudowa ma mieć możliwość zamontowania w szafie 19".
17. Zasilanie z sieci 230V/50Hz.
18. Musi istnieć możliwość konfiguracji urządzenia poprzez terminal i linię komend oraz konsolę graficzną (GUI). Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone poprzez szyfrowanie komunikacji.
19. Musi być zapewniona możliwość definiowania wielu administratorów o różnych uprawnieniach. System powinien umożliwiać aktualizację oprogramowania oraz zapisywanie i odtwarzanie konfiguracji z pamięci USB.
20. Jednocześnie, dla systemu bezpieczeństwa powinna być dostępna zewnętrzna sprzętowa platforma centralnego zarządzania pochodząca od tego samego producenta.
    - System powinien mieć możliwość współpracy z zewnętrznym, sprzętowym modułem centralnego zarządzania umożliwiającym m. in.:
    - Przechowywanie i implementację polityk bezpieczeństwa dla urządzeń i grup urządzeń z możliwością dziedziczenia ustawień po grupie nadrzędnej.
    - Wersjonowanie polityk w taki sposób, aby w każdej chwili dało się odtworzyć konfigurację z dowolnego punktu w przeszłości.
    - Zarządzanie wersjami firmware'u na urządzeniach oraz zdalne uaktualnienia.
    - Zarządzenie wersjami baz sygnatur na urządzeniach oraz zdalne uaktualnienia.
    - Monitorowanie w czasie rzeczywistym stanu urządzeń (użycie CPU, RAM).
    - Zapis i zdalne wykonywanie skryptów na urządzeniach.
21. Serwis oraz aktualizacje: Dostawca powinien dostarczyć licencje aktywacyjne dla funkcji bezpieczeństwa na okres 5 lat, System powinien być objęty serwisem gwarancyjnym producenta przez okres 5 lat.
22. Wymiary maksymalne (HxWxL), 5 cm x 33 cm x 26 cm, maksymalna waga: 3 kg
23. Maksymalny pobór mowy w trybie pracy: 150 W

Rys 4.7a Przykładowe urządzenie bezpieczeństwa dostępu do internetu Typu B

5. Wyposażenia Telecentrum

W ramach projektu Rozwój społeczeństwa informacyjnego w Czeladzi planowane jest uruchomienie dwóch telecentrów umieszczonych w następujących lokalizacjach:

- Centrum Edukacyjno-Społeczne PIASKI, Czeladź, ul. Zwycięstwa 6
- Centrala Miejskiej Biblioteki Publicznej, Czeladź, ul. 1 Maja 27

Telecentra zapewnią stały, szerokopasmowy dostęp do sieci Internet oraz możliwość korzystania z usług takich jak drukowanie czy też nagrywanie płyt CD i DVD. Dodatkowo, klienci telecentrów będą mogli korzystać z możliwości skanowania dokumentów i zdjęć wraz z ich obróbką przy pomocy standardowego oprogramowania. Telecentra zapewnią również dostęp do usług publicznych on-line, dostęp do stron urzędowych, portali regionalnych, kulturalnych, mogą w przyszłości stać się centrami edukacji umożliwiającymi ich użytkownikom podnoszenie kwalifikacji z wykorzystaniem metod e-learningowych. Planowane telecentra zostaną wyposażone w nowoczesny sprzęt komputerowy, oprogramowanie oraz urządzenia i rozwiązania zapewniające akceptowalny poziom bezpieczeństwa informatycznego oraz ochrony antywirusowej.

Urządzenia przewidziane do zastosowania w telecentrach:

Lp.	Urządzenie/Element	Ilość
1	Stanowiska komputerowe	12
2	Przełącznik 24portowy	2
3	Urządzenie bezpiecznego dostępu do internetu TYP A	2
4	Stanowisko operatora	2
5	Skaner A3	2
6	Drukarka laserowa kolor A4 sieciowa	2
7	Drukarka laserowa mono A4 sieciowa	2

5.1.1. Stanowiska komputerowe

Każde stanowisko komputerowe zostaje wyposażone w komputer klasy PC o parametrach nie gorszych od:

Lp.	Podzespół	Parametr/Opis
1	Procesor	Dwurdzeniowy, Częstotliwość rdzenia 2.4GHz, Częstotliwość magistrali 800MHz, 3MB cache
2	Obudowa	Typu Tower
3	Pamięć RAM	Taktowanie 1066MHz DDR 2GB
4	Dysk Twardy HDD	250GB, cache 16MB SATAII
5	Naped Optyczny	DVD+/-RW z oprogramowaniem
6	System operacyjny	Microsoft Windows XP PRO SP3
7	Oprogramowanie	Microsoft Office 2007 Pro
8	Karta sieciowa	10/100 Mb/s
9	Karta graficzna	Zintegrowana 256MB
10	Monitor	LCD 19" rodzaj matrycy TN czas reakcji 5ms kontrast 1:1000 jasność 300cd/m2 ilość wyświetlanych kolorów 16,7m kąt widzenia 160H/160V
11	Płyta główna	Częst. magistrali pamięci 1333MHz Możliwość do rozbudowy pamięci 4GB 1xPCI-Express x16; 2x PCI-Express x1; 8 x USB 2.0/1.1 1 x PS/2 port klawiatury 6x analogowe wyjście

W każdym telecentrum projektuje się zastosowanie stanowiska operatora, którego parametry nie powinny być gorsze od następujących:

Lp.	Podzespół	Parametr/Opis
1	Procesor	Czterordzeniowy, Częstotliwość rdzenia 2.5 GHz, Częstotliwość magistrali 1333MHz, 3MB cache
2	Obudowa	Typu Tower

3	Pamięć RAM	Taktowanie 1333MHz DDR 4GB
4	Dysk Twardy HDD	2x250GB, cache 16MB SATAII
5	Napęd Optyczny	DVD+/-RW z oprogramowaniem
6	System operacyjny	Microsoft Windows Serwer 2008 Standard
7	Karta sieciowa	10/100 Mb/s
8	Karta graficzna	Zintegrowana
9	Monitor	LCD 19" rodzaj matrycy TN czas reakcji 5ms kontrast 1:1000 jasność 300cd/m2 ilość wyświetlanych kolorów 16,7m kąt widzenia 160H/160V
10	Płyta główna	Częst. magistrali pamięci 1333MHz Możliwość do rozbudowy pamięci 16GB 1xPCI-Express x16; 2x PCI-Express x1; 8 x USB 2.0/1.1 1 x PS/2 port klawiatury 6x analogowe wyjscie

5.1.2. Przełącznik sieciowy

Dostawa i wdrożenie przełączników dystrybucyjnych w telecentrach.
Przełącznik Typu A:

Specyfikacja techniczna przełącznika sieciowego L2 – 24 interfejsy Gigabit Ethernet została przedstawiona w podpunkcie 3.5.

5.1.3. Urządzenie bezpiecznego dostępu do Internetu - Gateway

Kluczowym elementem systemu zabezpieczeń sieci telecentrów będzie wielofunkcyjny system bezpieczeństwa klasy UTM składający się z następujących komponentów funkcjonalnych:

- Firewall klasy Stateful Inspection
- Antivirus
- System detekcji i prewencji włamań (IDP)

- VPN, zgodny z IPSec, PPTP i L2TP oraz SSL- VPN
- Antyspam
- Filtracja stron www
- Kontrola pasma (Traffic Management)

Każdy Infokiosk, niezależnie od przeznaczenia i sposobu montażu, zostanie wyposażony w gateway o funkcjonalności i minimalnych wymaganiach technicznych, przedstawionych poniżej (TYP A, razem 2 szt.). Gateway zostanie zintegrowany mechanicznie z obudową Infokiosku i programowo z jego jednostką centralną.

Element bezpieczeństwa UTM ma zapewnić następującą funkcjonalność (dot. TYP A):

- Blokowanie prób nieupoważnionego dostępu zgodnie z ustaloną polityką bezpieczeństwa (kontrola i ograniczenie dostępu do sieci wewnętrznej)
- Inspekcja ruchu sieciowego na wielu poziomach (m.in. firewall prowadzi kontrolę na podstawie adresów IP, kierunku i stanu połączeń, protokołów i aplikacji, indywidualnych użytkowników)
- Tworzenie stref bezpieczeństwa i modelowanie charakterystyki ruchu między nimi.
- Szybkie powiadamianie administratorów w sytuacjach wyjątkowych (np. poprzez alarm na konsolę lub e-mail).
- Gromadzenie logów o zaistniałych zdarzeniach oraz zapewnienie możliwości tworzenia statystyk i raportów.
- Wykrywanie i blokowanie penetracji i ataków wykonywanych przez intruzów i robaki internetowe za pomocą wielu metod detekcji Wykrywanie ataków (D) DoS przez sygnatury i analizę ruchu sieciowego (przekroczenie wartości progowych).
- Funkcjonalność antywirusowa zaimplementowana w oparciu o sprzętowy akcelerator (ASIC) .
- Skanowanie antywirusowe protokołów HTTP, FTP, POP3, IMAP i SMTP
- Skanowanie AV zarówno na bazie sygnatur jak i heurystycznie
- Obsługa NAT dla VPN

- Moduł antyspamowy w obrębie protokołów SMTP, POP3 i IMAP bazujący na wielu czynnikach, takich jak:
  - sprawdzenie zdefiniowanych przez administratora adresów IP przez które przechodził mail,
  - sprawdzenie zdefiniowanych przez administratora adresów pocztowych,
  - RBL, ORDBL
  - Sprawdzenie treści pod kątem zadanych przez administratora słów kluczowych
- Moduł filtracji stron www filtrujący na bazie:
  - białej i czarnej listy URL
  - W oparciu o zawarte w stronie słowa kluczowe
  - Javy, cookies i ActiveX
- Urządzenie musi wspierać różne poziomy i domeny uprawnień dla administratorów

Dostarczony sprzęt musi być objęty 5 letnią gwarancją. Dodatkowo wykonawca dostarczy w ramach zamówienia subskrypcję szczepionek (wszelkie aktualizacje), w zakresie Firewall klasy Stateful Inspection, Antywirus, System detekcji i prewencji włamań (IDP), VPN (zgodny z IP Sec, PPTP i L2TP oraz SSL- VPN), Antyspam, Filtracja stron www, Kontrola pasma (Traffic Management), na okres 5lat.

5.1.4. Urządzenia typu: drukarka, skaner

Skanery A3 oraz drukarki będące na wyposażeniu telecentrów muszą posiadać parametru nie gorsze od:

Tabela 5.1.4a Parametry skanerów i drukarek.

Lp.	Podzespół	Parametr/Opis
1	Skaner A3	Optyczna rozdzielczość skanera 1200x1200dpi Głębia kolory 48bit Obszar skanowania 420mm V oraz 297mm H Interfejs USB 2.0 Współpraca z systemami operacyjnymi MAC OS X; Windows XP, Windows Vista lub nowszy

		Gwarancja 24miesiące
2	Drukarka laserowa kolor A4 sieciowa	Rozdzielczość kolor 600x600dpi Rozdzielczość mono 600x600dpi Zainstalowana pamięć 64MB Prędkość procesora 360MHz Interfejsy:1xUSB2.0 1 x sieć - Ethernet 10Base-T/100Base-TX - RJ-45 Normowane obciążenie 2000str/mies Współpraca z systemami operacyjnymi MAC OS X; Windows 2000; Windows XP, Windows Vista lub nowszy
3	Drukarka laserowa mono A4 sieciowa	Rozdzielczość mono 600x600dpi Zainstalowana pamięć 64MB Prędkość procesora 360MHz Interfejsy:1xUSB2.0 1 x sieć - Ethernet 10Base-T/100Base-TX - RJ-45 Normowane obciążenie 2000str/mies Współpraca z systemami operacyjnymi MAC OS X; Windows 2000; Windows XP, Windows Vista lub nowszy

6. System logowania do hot spotów

6.1. Wymagania minimalne dla systemu Wi-Fi

Zakłada się zastosowanie radiowego punktu dostępowego o parametrach minimalnych, przedstawionych poniżej

Tabela 6.1a Parametry routerów bezprzewodowych Wi-Fi.

Lp.	**Element konfiguracji**	**Wymagania minimalne**
1	Standard	IEEE 802.11b/g
2	Tryb pracy radiowej	802.11b+g, 802.11b only, 802.11g only
3	Szerokość kanału	20MHz
4	Transfer Danych	802.11g: 54Mbit/s

5	Interfejsy	WAN	Ethernet 10/100 (RJ-45)
		LAN	4x Ethernet 10/100 (RJ-45) IEEE 802.11b/g
6	Zarządzanie	konfiguracja przez przeglądarkę WWW - lokalna oraz zdalna,	
7	Adresacja	Server / klient DHCP	
8	Bezpieczeństwo	WPA	
		WEP 128bit	
		Secure Easy Setup	
		Firewall	
9	Jakość Usług	ustawianie priorytetu (niski / wysoki) dla dwóch, dowolnie wybranych urządzeń w sieci LAN (po adresie MAC),	
10	Standardy	802.3af 802.1q 802.11g	
11	Zasilanie	**PoE**	
		AC	90- 250V, 48-62Hz
		DC	42-60V

6.2. Zarządzanie systemem WLAN

Usługi dotyczące użytkowników:

- rejestracje użytkowników z wypełnieniem formularza poprzez stronę www lub przez wybraną osobę,
- baza użytkowników i zarządzanie kontami użytkowników,
- logowanie użytkowników,
- blokowanie użytkowników (czasowe lub stałe).

Usługi dotyczące sesji:

- limity pobierania/wysyłania (QoS) dla każdego klienta (np. 144kbps, 256kbps);
- ograniczenia dostępności do zasobów (np. 30 min);

- przekierowywanie użytkownika po zalogowaniu na zdefiniowaną stronę www;
- powrót do strony logowanie po zdefiniowanym czasie;
- oddzielne reguły (firewall) dla klienta;
- możliwość ustawienia limitu czasowego dotyczący sesji użytkownika;
- możliwość ograniczania ruch przed i po zalogowaniu;
- auto wylogowanie (gdy użytkownik jest niedostępny w sieci dłużej niż xxx czasu);

Usługi dotyczące sprzętu:

- monitoring urządzeń;
- administrowanie urządzeniami poprzez dostęp zdalny;
- powiadomienia o awariach (sms, e-mail);
- monitoring serwera;
- monitoring łącza internetowego WAN;

Wsparcie techniczne:

- użytkownikowi odnośnie konfiguracji urządzenia do pracy w sieci;
- pomoc telefoniczna w zdefiniowanych godzinach;
- pomoc mailowa – zgłoszenia użytkowników pod wskazany adres email;
- rejestracja zgłoszeń użytkowników poprzez stronę www;
- raportowanie zgłoszonych awarii i problemów (cykliczne, na żądanie):

Inne usługi:

- statystyki:
  - pobrane/wysłane dane;
  - podział na godziny, dni, tygodnie, miesiące, etc;
  - podział na hotspot, użytkowników;
- przeglądane strony (po domenie, hostcie);
- filtr „rodzicielski" (blokowanie nieporządnych stron);
- „captive portal" - przekierowanie na stronę/portal przed zalogowaniem (np. strona Urzędu Miasta Czeladź;

7. Projekt logiczny

7.1. Opis zamierzenia – zakres projekt

W ramach projektu pn. „Rozwój społeczeństwa informacyjnego w Zagłębiu Dąbrowskim – Czeladź" przewiduje się budowę infrastruktury teletechnicznej, której wydzielone elementy zostaną zabudowane w istniejącej serwerowni Urzędu Miasta Czeladź przy ulicy Katowicka 45 w Czeladzi.

Zakres niniejszego projektu obejmuje dostawę, instalację i konfigurację:

1) Radiolinia
2) Stacja Bazowa WiMAX
3) Serwer Zarządzania
4) Serwer Aplikacji
5) Przełącznika sieciowego
6) Urządzenia bezpiecznego dostępu do internetu – Gateway
7) Stanowisko operatora

wraz z niezbędnym oprogramowanie systemowym, użytkowym i zarządzającym. Gwarancja urządzeń oraz niezbędnych licencji do oprogramowania przewidziana na 5 lat.

7.2. Konfiguracja urządzeń

Na potrzeby projektu zastosowana następujące nazwy urządzeń:

Nazwa	**Opis**
Switch A	Przełącznik sieciowy
R1	Wyposażenie radiolinii nr1

R2	Wyposażenie radiolinii nr2
SB1	Stacja Bazowa nr 1
Serwer NMS	Serwer zarządzania radiem
Serwer AP	Serwer aplikacji
Gateway	Urządzenie bezpieczeństwa dostępu do sieci
SO	Stanowisko Operatora

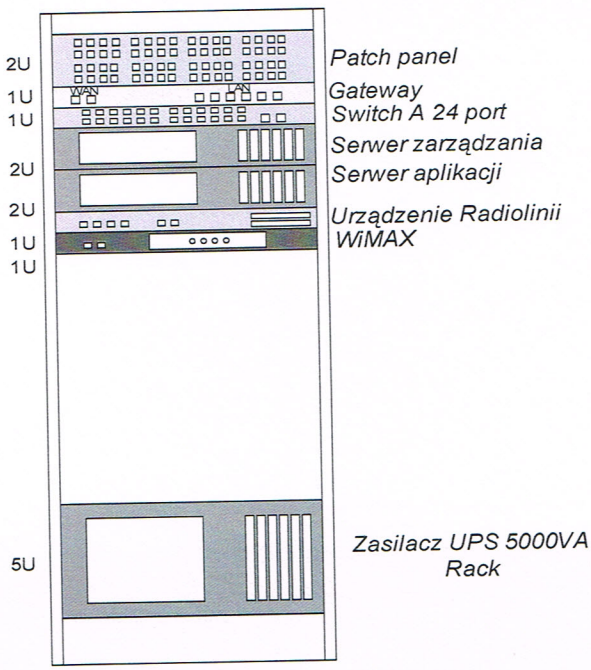
Sposób połączenia urządzeń, topologia fizyczna i logiczna

1. Połączenia między wyposażeniem Centrum Zarządzania

Nazwa	**Opis**
Łącze operatora	Gateway (WLAN G2/1) (przewód UTP)
Gateway (LAN G6/1) (przewód UTP)	Router 1 (WLAN G2/1)
Switch A(24/3)	R1 (eth0)
Switch A(G24/4)	R1 (eth1) - zarządzanie
Switch A(G24/5)	SB1 (eth0)
Switch A(G24/6)	SB1 (eth1) - zarządzanie
Switch A(G24/7)	Infokiosk (eth0)
Switch A(G24/8)	Router WiFi(eth0)
Switch A(G24/20)	SO (eth0)
Switch A(G24/11)	NMS (eth0)
Switch A(G24/12)	AP (eth0)

Oznaczenia typu interfejsu w powyższych tabelach

– Gx/y, eth – interfejs miedziany typu Ethernet



Rys.7.2a Rozmieszczenie urządzeń w szafie teletechnicznej w Centrum Zarządzania

Połączenia pomiędzy portami urządzeń radiolinii a switchem A są realizowane jako połączenia trunkowe zgodne ze standardem IEEE 802.1Q. Standard 802.1Q przenoszący VLANy jest konieczny do obsługi sieci, w tym VLAN zarządzający, który obsługiwany jest przez Urząd.

7.3. VLANy, adresacja IP

W celu usprawnienia procesu zarządzania poszczególnymi elementami sieci zakłada się utworzenie wirtualnych sieci VLAN. Proces ten konieczny jest do scentralizowania i uproszczenia zarządzania tymi elementami. Zakład się utworzenie następujących VLANów, których nazwy powstają wg schematu:

VLAN 100 – oznaczenie VLANu obejmującego radiolinie,

VLAN 101 – oznaczenie VLANu obejmującego zarządzanie radioliniami,

VLAN 200 – oznaczenie VLANu obejmującego Stacje Bazowe WiMAX,

VLAN 201 – oznaczenie VLANu obejmującego zarządzanie Stacjami Bazowymi WiMAX,

VLAN 400 - oznaczenie VLANu obejmującego Infokioski zewnętrzne i wewnętrzne,

VLAN 500 – oznaczenie VLANu obejmującego urządzenia dostępowe Wi-Fi

VLAN 600 – oznaczenie VLANU obejmującego Infokioski

Na potrzeby zarządzania radioliniami przeznaczone są osobne interfejsy fizyczne wg powyższej tabeli. Połączenie z systemem zarządzania radioliniami będzie odbywało się poprzez porty dostępowe Switcha A odpowiednio dla serwera aplikacji AP.

Interfejsy zarządzające Switcha A, Routera 1, Gatewaya oraz serwerów NMS i AP będą objęte VLANami zarządzającymi Urzędu:

VLAN 110 – zarządzanie: switch, router, gateway

VLAN 120 – zarządzanie serwerami

Adresy IP punktów infokiosków.

Punkty terminali abonenckich są adresowane według poniższego schematu:

192.168.100.[x+10] – maska wynosi 24-bitów – x oznacza numer urządzenia abonenckiego systemu WiMAX. Wszystkie urządzenia abonenckie należą do tej samej sieci VLAN.

Adresy strumieni danych z infokiosków są tworzone wg schematu:

192.168.110.[y+10] – gdzie y oznacza nr infokiosku;

Adresy Strumieni danych z/do punktów dostępowych typu Hot Spot (rutery wewnętrzne) są tworzone wg schematu:

192.168.120.[x+10] – gdzie x oznacza numer punktu infokiosku

Adresy Strumieni danych z/do punktów dostępowych typu Hot Spot (rutery zewnętrzne montowane przy urządzeniach abonenckich) są tworzone wg schematu:

192.168.121.[x+10] – gdzie x oznacza numer punktu infokiosku

Zarządzenie radioliniami odbywa się poprzez adresy z puli 192.168.0.0/24 – dokładne adresy będą umieszczona w tabeli poniżej

Adresy VLANów zarządzających Urzędu:

VLAN 110 – 192.168.10.0/24

VLAN 120 - 192.168.20.0/24

8. Planowanie Radiowe

8.1. Kanały radiowe systemu WiMAX

Tabela 8.1a Zarezerwowane kanały radiowe dla systemy WiMAX

Nr kanału	Pasmo UL [MHz]	Pasmo DL [MHz]
Kanał 21	3672,75	3772,75
Kanał 22	3676,25	3776,25
Kanał 23	3679,75	3779,75
Kanał 24	3683,25	3783,25

W celu zwiększenia wydajności i efektywniejszego wykorzystania kanałów radiowych dla systemu WiMAX projektuje się aby cztery kanały radiowe 3,5MHz zostają połączone w dwa kanały 7Mhz.

Tabela 8.1b Zarezerwowane kanały radiowe dla systemy WiMAX

Nr kanału o szerokości 7MHz	Nr kanału o szerokości 3,5MHz	Pasmo UL [MHz] kanału 7MHz	Pasmo DL [MHz] kanału 7MHz
Kanał 1	Kanał 21	3672,75	3772,75
	Kanał 22		
Kanał 2	Kanał 23	3679,75	3779,75
	Kanał 24		

8.2. Obliczenie maksymalnego zasięgu stacji bazowej systemu WiMAX

Założenia wstępne:

Lp.	Parametr	Wartość
1	Modulacja	BPSK, QPSK, 16QAM, 64QAM
2	Polaryzacja	V
3	Częstotliwość	3,6 GHz
4	Metoda dostępu	TDD TDMA

5	Strefa klimatyczna (podział wg ITU)	H
6	Intensywność opadu deszczu $R_{0,1}$	10 [mm/h]
7	Dostępność łączy w skali roku w związku z warunkami atmosferycznymi	99,9%
8	Antena stacji bazowej	90° AZ, 7° EL
9	Antena stacji terminalowej	20° AZ, 20° EL
10	Zysk anteny stacji bazowej G_B	14,5 dBi
11	Zysk anteny stacji terminalowej G_T	16,5 dBi
12	Czułość odbiornika dla modulacji 64QAM 3/4	-82 dBm
13	Czułość odbiornika dla modulacji 64QAM 2/3	-83 dBm
14	Czułość odbiornika dla modulacji 16QAM 3/4	-88 dBm
15	Czułość odbiornika dla modulacji 16QAM 1/2	-91 dBm
16	Czułość odbiornika dla modulacji QPSK 3/4	-94 dBm
17	Czułość odbiornika dla modulacji QPSK 1/2	-97 dBm
18	Czułość odbiornika dla modulacji BPSK 3/4	-98 dBm
19	Czułość odbiornika dla modulacji BPSK 1/2	-100 dBm
20	Moc nadajnika po stronie terminala stacji bazowej P_B	28 dBm
21	Moc nadajnika po stronie terminala abonenckiego P_T	20 dBm
22	Intensywność opadu deszczu $R_{0,1}$	10 [mm/h]

Obliczenie maksymalnego zasięgu stacji bazowej, dla dostępności systemu 99,9% dla polaryzacji V przy modulacji 64QAM dla anteny terminalowej.

Zaniki związane z tłumieniem na hydrometeorach

- Długość trasy d = 29 km,
- Tłumienie wolnej przestrzeni L = 132,81 dB,
- Tłumienie właściwe trasy $\gamma_R = k\, R_{0,1}^{\alpha} = 0,01$ dB/km,
- Efektywna długość trasy radiowej na której może wystąpić opad deszczu
- $D = d/(1+(d/(35*EXP(-0,015*\ R_{0,1}))))$ = 14,78 km,
- Tłumienie trasy propagacji na hydrometrach przekraczane w ciągu P = 0,1% czasu

$A_{0,1} = \gamma_R\, D = 0,103$ dB

Bilans mocy

Moc sygnału na wejściu odbiornika stacji bazowej

$P_{inB} = P_T + G_T - L + G_B = 20 + 16,5 - 132,81 + 14,5 = -81,81$ dBm

Moc sygnału na wejściu odbiornika stacji terminalowej

$P_{inT} = P_B + G_B - L + G_T = 28 + 14,5 - 132,81 + 16,5 = -73,81$ dBm

Margines zaniku dla mniejszej wartości mocy sygnału przy modulacji 64QAM

$A_z = P_{min} - P_{inB} = 82 - 81,81 = 0,19$ dB

Podsumowanie

Czułość odbiornika zarówno stacji bazowej jak i terminalowej dla modulacji 64 QAM ¾ wynosi -82 dBm. Dla odległości rzędu 29 km pomiędzy stacją bazową a stacją terminalową sygnał ze stacji terminalowej dotrze do stacji bazowej według powyższych wyliczeń na poziomie -81,81 dBm. W związku z powyższym pozostaje jeszcze margines zapasu sygnału na poziomie 0,19 dBm aby odbiornik mógł pracować dalej z modulacją 64 QAM ¾.

Na podstawie wyliczeń związanych z tłumiennością sygnału na hydrometeorach, tłumienie fali elektromagnetycznej o częstotliwości 3,6 GHz na odległości 29 km przez opad deszczu wynosi 0,10 dB. Biorąc pod uwagę zapas sygnału na poziomie 0,19 dBm oraz tłumienie wywołane opadami deszczu na poziomie 0,10 dB, istnieje możliwość pracy stacji bazowej i odbiornika na modulacji 64 QAM do 29 km.

Dobór modulacji dla najbardziej wysuniętych punktów infokiosków

1)Odległość PI-06 od Stacji Bazowej przy ulicy Miasta Auby 4

Odległość od stacji bazowej	Tłumienie wolnej przestrzeni
970m	103,067

Obliczenie maksymalnego zasięgu stacji bazowej, dla dostępności systemu 99,9% dla polaryzacji V przy modulacji 64QAM ¾ dla anteny terminalowej.

Zaniki związane z tłumieniem na hydrometeorach

- Długość trasy d = 0,97 km,
- Tłumienie wolnej przestrzeni L = 102,28 dB,
- Tłumienie właściwe trasy $\gamma_R = k R_{0,1}^{\alpha} = 0,00702$ dB/km,
- Efektywna długość trasy radiowej na której może wystąpić opad deszczu
- D =d/(1+(d/(35*EXP(-0,015* $R_{0,1}$)))) = 0,94 km,
- Tłumienie trasy propagacji na hydrometrach przekraczane w ciągu P = 0,1% czasu

$A_{0,1} = \gamma_R D = 0,0066$ dB

Bilans mocy

Moc sygnału na wejściu odbiornika stacji bazowej

$P_{inB} = P_T + G_T - L + G_B = 20 + 16,5 - 102,81 + 14,5 = -51,28$ dBm

Moc sygnału na wejściu odbiornika stacji terminalowej

$P_{inT} = P_B + G_B - L + G_T = 28 + 14,5 - 102,81 + 16,5 = -43,28$ dBm

Margines zaniku dla mniejszej wartości mocy sygnału przy modulacji 64QAM

$A_z = P_{min} - P_{inB} = 82 - 51,28 = 30,71$ dB

W związku z powyższym pozostaje jeszcze margines zapasu sygnału na poziomie 30,71 dBm aby odbiornik mógł pracować dalej z modulacją 64 QAM ¾.

2)Odległość PI-13 od Stacji Bazowej przy ulicy Miasta Auby 4

Odległość od stacji bazowej	Tłumienie wolnej przestrzeni
690m	103,067

Obliczenie maksymalnego zasięgu stacji bazowej, dla dostępności systemu 99,9% dla polaryzacji V przy modulacji 64QAM ¾ dla anteny terminalowej.

Zaniki związane z tłumieniem na hydrometeorach

- Długość trasy d = 0,69 km,
- Tłumienie wolnej przestrzeni L = 99,32 dB,
- Tłumienie właściwe trasy $\gamma_R = k\ R_{0,1}^{\alpha} = 0,00702$ dB/km,
- Efektywna długość trasy radiowej na której może wystąpić opad deszczu
- D =d/(1+(d/(35*EXP(-0,015* $R_{0,1}$)))) = 0,67 km,
- Tłumienie trasy propagacji na hydrometrach przekraczane w ciągu P = 0,1% czasu

$A_{0,1} = \gamma_R\ D = 0,00474$ dB

Bilans mocy

Moc sygnału na wejściu odbiornika stacji bazowej

$P_{inB} = P_T + G_T - L + G_B = 20 + 16,5 - 199,32 + 14,5 = -48,32$ dBm

Moc sygnału na wejściu odbiornika stacji terminalowej

$P_{inT} = P_B + G_B - L + G_T = 28 + 14,5 - 102,81 + 16,5 = -40,32$ dBm

Margines zaniku dla mniejszej wartości mocy sygnału przy modulacji 64QAM

$A_z = P_{min} - P_{inB} = 82 - 51,28 = 33,68$ dB

W związku z powyższym pozostaje jeszcze margines zapasu sygnału na poziomie 33,68 dBm aby odbiornik mógł pracować dalej z modulacją 64 QAM ¾.

8.3. Tabela z wynikami

W poniższej tabeli (Tabela nr 5) zamieszczone są zbiorcze informacje tj. odległość punktu Infokiosku od stacji bazowej, rodzaj zastosowanej modulacji, dotyczące planowania radiowego jakie przewiduje się zastosować przy rozwoju informatycznego społeczeństwa miasta Czeladź

Tabela 8.3a. Rodzaje zastosowanych modulacji anten WiMAX dla poszczególnych punktów PI.

Punkt kamerowy	Odległość od stacji bazowej [m]	Wybór trybu modulacji
PI-01	200	64QAM
PI-02	310	64QAM
PI-03	102	64QAM
PI-04	522	64QAM
PI-05	260	64QAM
PI-06	970	64QAM
PI-07	350	64QAM
PI-08	470	64QAM
PI-09	600	64QAM
PI-10	170	64QAM
PI-11	220	64QAM
PI-12	90	64QAM
PI-13	690	64QAM
PI-14		
PI-15	400	64QAM

9. Pomiary

Przed oddaniem systemu Stacji Bazowych dla miasta Czeladź na terenie miasta Czeladź do eksploatacji należy wykonać pomiary:

– uziemienia technologicznego (po wykonaniu uziemień należy sprawdzić spełnienie wymogu : Ruz max =< 3 W) ,

– skuteczność ochrony przed porażeniem prądem elektrycznym ,

– ochrony odgromowej ,

– stanu izolacji ,

– rozkładu natężenia PEM dla celów ochrony ludzi i środowiska ,

– rozkładu natężenia PEM dla celów BHP .

– Komplet dokumentacji pomiarowej (powykonawczej i protokoły pomiarowe) należy przekazać do:

Pracownia Projektowo- Usługowa Bogusław Dyduch, 54-104 Wrocław, ul. Kozia 7a/2

Firma SoftBlue, 85-047 Bydgoszcz, ul. B. Chrobrego 24 lol nr 1

10.Zalecenia i Normy

Poniżej zestawiono zestaw zaleceń i norm, zgodnie z którymi należy postępować podczas realizacji projektu pn. „Rozwój społeczeństwa informacyjnego w Zagłębiu Dąbrowskim - Czeladź", przeprowadzania procedury odbiorowej oraz wykonywania dokumentacji powykonawczej.

- PN-E-05100-1 „Elektroenergetyczne linie napowietrzne. Projektowanie i budowa"
- PN-EN 50173-1:2007 (U) Technika informatyczna - Systemy okablowania strukturalnego - Część 1: Wymagania ogólne.
- PN-EN 50173-2:2007 (U) Technika informatyczna - Systemy okablowania strukturalnego - Część 2: Lokale biurowe
- PN-EN 50174-1:2002 Technika informatyczna - Instalacja okablowania - Część 1: Specyfikacja i zapewnienie jakości.
- PN-EN 50174-2:2002 Technika informatyczna - Instalacja okablowania - Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków
- PN-EN 50174-3:2005 Technika informatyczna - Instalacja okablowania - Część 3: Planowanie i wykonawstwo instalacji na zewnątrz budynków.
- PN-EN 50346:2004 Technika informatyczna - Instalacja okablowania - Badanie zainstalowanego okablowania.
- PN-ISO/IEC 2382-25:1996 Technika informatyczna - Terminologia - Lokalne sieci komputerowe.
- ZN-02/TD S.A. - 01 Projektowanie i budowa sieci telekomunikacyjnej - Ogólne zasady projektowania i budowy sieci kablowych.
- ZN-02/TD S.A. - 01/2 Projektowanie i budowa sieci telekomunikacyjnej - Ogólne zasady projektowania i budowy sieci kablowych - Dokumenty normatywne.
- ZN-02/TD S.A. - 01/3 Projektowanie i budowa sieci telekomunikacyjnej - Ogólne zasady projektowania i budowy sieci kablowych - Ogólne zasady projektowania i budowy sieci kablowych.
- ZN-02/TD S.A. - 01/4 Projektowanie i budowa sieci telekomunikacyjnej - Ogólne zasady projektowania i budowy sieci kablowych - Zasady oznaczania i znakowania elementów sieci kablowych.

- ZN-02/TD S.A. - 05 Budowa sieci dostępowych miedzianych

11.Spis załączników

Do niniejszego opracowania dołączono następujące załączniki:

- karty lokalizacyjne Infokiosków,
- tabela lokalizacji punktów Infokiosków,
- tabela lokalizacji węzłów szkieletowych,
- okablowanie węzłów szkieletowych oraz punktów dostępowych,
- okablowani punktów dostępowych w oparciu o sieć światłowodową,
- sposób prowadzenia okablowania w punktach objętych inwestycją,
- karta gwarancyjna,
- specyfikacja techniczna odbioru robót budowlanych,
- inwentaryzacja Urzędu Miasta (UM-01 – UM-04),
- schemat ideowy połączeń w węzłach szkieletowych (M-00 – M-03),
- schemat ideowy połączeń w puntach Infokiosków (M-00 – M-03),
- karty katalogowe przykładowych materiałów, urządzeń.

Wykaz skrótów:

BHP – Bezpieczeństwo Higieny Pracy

BPSK – Dwuwartościowa modulacja fazowa

IP – Adres IP (Internet Protocol) w wersji 4

NMS – System zarządzania siecią

PI - Punkt infokiosku

PEM – Promieniowanie elektromagnetyczne

PSK- Modulacja fazy

SA – Serwer aplikacji

SB – Stacja Bazowa systemu WiMAX

SO – Stanowisko operatora

SR – Stacja retransmisyjna

SZ – Serwer zarządzania

TCP – Protokół transportowy

UA - Urządzenie abonenckie (Terminal Abonencki) systemu WiMAX

QAM – Kwadraturowa modulacja amplitudowo-fazowa

QPSK – Czterowartościowa modulaja fazy

UA- Urządzenie Abonenckie

WS – Węzeł szkieletowych