4.2. Opis alternatywnych wariantów, analiza opcji.

Poniżej poddano analizie najistotniejsze z przedstawionych powyżej elementów projektu. Omówiono obszary, zdaniem autorów opracowania, najważniejsze z punktu widzenia analizy alternatywnych rozwiązań. Przykładem jest tu analiza technologii wybranej dla implementacji rozwiązania sieci teleinformatycznej czy też powody, dla których zdecydowano się na wybór telefonii VoIP dla modernizacji systemu łączności telefonicznej w Urzędzie.
Niektóre z elementów projektu pominięto w tej analizie ze względu na oczywistość wyboru. Dla przykładu, zdaniem autorów nie było sensu omawiać przyczyn wyboru technologii wykonania procesorów zastosowanych w serwerach czy też komputerach PC, ze względu na dominację rynkową procesorów typu CISC (do tej grupy należą miedzy innymi procesory firmy Intel oraz AMD) nad procesorami typu RISC oraz zdecydowaną i oczywistą różnicę cenową.

Analiza możliwości technicznych dla zabezpieczenia sieci

Według badań magazynu InformationWeek oraz firmy konsultingowej Accenture, w 2006 blisko 57% firm doświadczyło problemów z wirusami komputerowymi, 34% z robakami, 18% padło ofiarą ataków DoS, 9% doświadczyło włamań sieciowych, a 8% padło ofiarą kradzieży tożsamości. Dzieje się tak mimo wydatków na bezpieczeństwo sięgających 10% całkowitego budżetu IT.
Mając powyższe na uwadze wydaje się niekwestionowanym, konieczność poniesienia wydatków na zabezpieczenie sieci teleinformatycznej oraz aplikacji użytkowanych w Łódzkim Centrum Kontaktu z Mieszkańcami.
Istnieją dwa podstawowe nurty w walce z zagrożeniami bezpieczeństwa.
Pierwszym z nich jest możliwie skuteczne zapobieganie powstawaniu takich usterek. Chociaż wyeliminowanie błędów zabezpieczeń w skomplikowanych systemach teleinformatycznych jest w praktyce niemożliwe (lub przynajmniej nieekonomiczne), znanych jest szereg metod, które pozwalają na zredukowanie ryzyka.
Drugą strategią zapewnienia bezpieczeństwa systemów teleinformatycznych jest budowanie ich w sposób, który ogranicza ewentualne problemy wynikające z naruszenia zabezpieczeń lub niepożądanej aktywności uprawnionego użytkownika. Takie podejście staje się szczególnie istotne w przypadku utrzymywania dużej infrastruktury o zastosowaniu komercyjnym, na

przykład w jednostkach administracji publicznej.

Ponieważ w omawianym projekcie bardzo trudne, a na pewno bardzo kosztowne, byłoby zastosowanie się do zasad występujących w pierwszym podejściu (np. trudności ze zmuszeniem do stosowania producentów oprogramowania norm Common Criteria ISO/IEC 15408, ITSEC czy FIPS), zdecydowano się na wybór podejścia polegającego na ograniczeniu zagrożeń. Jednym z ważniejszych narzędzi w tak pojętym zarządzaniu bezpieczeństwem jest ograniczanie do niezbędnego minimum zakresu możliwej interakcji między użytkownikami i systemami, oraz pomiędzy poszczególnymi komponentami platformy. Istnieją dwa argumenty przemawiające za taką praktyką: pierwszy mówi, że im mniejsza jest objętość kodu, z którą użytkownik lub inny system może bezpośrednio oddziaływać, tym statystycznie mniej błędów programistycznych może zostać wykorzystane. Drugi wskazuje, że gdy dojdzie do przełamania zabezpieczeń jednego z komponentów systemu, ogranicza to zbiór systemów, które mogłyby bezpośrednio paść ofiarą dalszych ataków, więc muszą stać się przedmiotem kosztownej i czasochłonnej analizy.

Czterema podstawowymi metodami ograniczenia zakresu interakcji są:

- dobrane do zastosowania, minimalistyczne projektowanie protokołów,
- unikanie łączenia diametralnie różnych funkcjonalności w ramach jednego rozwiązania;
- separacja komponentów logicznych platformy tak, by zdobycie uprawnień administratora na jednym komputerze nie oznaczało całkowitej utraty kontroli nad systemami;
- wyłączanie zbędnych usług sieciowych na platformach.

Stąd też decyzja o zastosowaniu zabezpieczeń przeciwwłamaniowych sieci w postaci firewall'a, serwera VPN oraz szyfrowania transakcji protokołem SSL. Najpopularniejszy w tej chwili bezpieczny sposób transmisji danych SSL opiera się na technologii RSA, kombinacji klucza publicznego i klucza prywatnego (informacje zakodowane przy pomocy klucza publicznego RSA mogą być odkodowane tylko z użyciem odpowiadającego mu klucza prywatnego. RSA to algorytm kryptograficzny o zmiennej długości, który szyfruje dane opierając się na formułach matematycznych).

Analiza możliwości technicznych dla telefonii

Technologia VoIP (Voice over Internet Protocol) jest alternatywą we współczesnej komunikacji. Pozwala na przeprowadzanie rozmów za pośrednictwem Internetu. Sygnał mowy jest poddany kompresji a następnie dzielony na pakiety i przesyłany za pomocą sieci. W węźle

odbiorczym taki proces zostaje odtworzony w odwrotnej kolejności, czego efektem jest otrzymanie normalnego sygnału mowy. Usługa taka pozwala na olbrzymie obniżenie kosztów rozmów w porównaniu z tradycyjną telefonią stacjonarną.

Zalety w porównaniu z telefonią tradycyjną:

- niezależność od operatorów/monopolistów państwowych (swoboda wyboru a potencjalnie także większa prywatność)
- często zerowy koszt połączeń VoIP
- niższy koszt połączeń z telefonią stacjonarną
- pełna mobilność użytkownika (problem roamingu ma ograniczone znaczenie)
- niski koszt infrastruktury (w porównaniu z tradycyjnymi liniami telefonicznymi)
- integracja z przyszłościowymi usługami takimi jak przesyłanie danych czy obrazu
- Wady w porównaniu z telefonią tradycyjną:
- większa zawodność usług
- konieczność posiadania dobrej jakości łącza internetowego
- przy realizacji sprzętowej większe koszty zakupu (np. aparatów) dla użytkownika końcowego

W kwietniu 2007 roku w Polsce było już 600 tysięcy użytkowników telefonii VoIP, a dalszych 2 mln deklarowało chęć korzystania z niej. Takie wyniki badań TNS Telecoms Index przedstawił TNS OBOP. 2/3 respondentów zainteresowanych usługami telefonii VoIP stwierdziło, że głównym powodem korzystania z telefonii internetowej jest cena połączeń (połączenia darmowe pomiędzy komputerami lub tańsze od standardowych w przypadku rozmów komputer – telefon).

W omawianym projekcie zdecydowano się na zaadaptowanie rozwiązania opartego o technologię VoIP, ponieważ wszystkie wymagane przez Projekt funkcjonalności telekomunikacyjne będą zaspokojone w takim samym stopniu jak w telefonii tradycyjnej, a koszty eksploatacji powinny być znacząco niższe.

4.2.1. Opis techniczny projektu.

W projekcie „Łódzkie Centrum Kontaktu z Mieszkańcami" przewiduje się realizację następującego zakresu rzeczowego:

1. Dostawa, instalacja i konfiguracja urządzeń do realizacji bezpiecznego styku z Internetem.
2. Dostawa, instalacja i konfiguracja serwerów wraz z zasobami masowymi.
3. Dostawa i instalacja sprzętu komputerowego na stanowiska „Łódzkiego Centrum Kontaktu z Mieszkańcami".
4. Dostawa, instalacja i konfiguracja systemu telefonii VoIP.
5. Zakup i wdrożenie oprogramowania narzędziowego i aplikacyjnego Wielokanałowej Platformy Usług Publicznych dla „Łódzkiego Centrum Kontaktu z Mieszkańcami".
6. Zakup i wdrożenie oprogramowania narzędziowego i aplikacyjnego Bazy Wiedzy o Usługach Publicznych.
7. Zakup i wdrożenie oprogramowania narzędziowego i aplikacyjnego Systemu Analiz Świadczonych Usług Publicznych.
8. Szkolenia z obsługi aplikacji i administrowaniem systemem.

Ad. 1. Bezpieczny styk z Internetem.

Niezbędnym elementem projektu „Łódzkie Centrum Kontaktu z Mieszkańcami" jest zapewnienie stabilnego i bezpiecznego sposobu komunikacji placówki ze światem zewnętrznym. Docelowo zakłada się podłączenie lokalizacji do dwóch niezależnych operatorów sieci Internet, tak by zapewnić bezprzerwowy dostęp do Centrum. W celu zapewnienia efektywnego działania systemów informatycznych „Łódzkiego Centrum Kontaktu z Mieszkańcami", konieczne jest zadbanie o właściwą organizację i wyposażenie sieci teleinformatycznej w urządzenia aktywne sieci teleinformatycznej. Dla niezawodnego i efektywnego połączenia wszystkich użytkowników koniecznym wydaje się zaprojektowanie sieci placówki w oparciu o następujące typy urządzeń:

- Router/Firewall – do zabezpieczenia dostępu z zewnątrz oraz zapewnienia obsługi funkcji bezpieczeństwa - szyfrowania danych, tunelowania oraz uwierzytelniania i autoryzacji użytkownika przy dostępie do sieci VPN,

- Przełącznik Ethernet – do podłączenia wszystkich urządzeń sieciowych i komputerowych wyposażonych w interfejsy sieciowe,
- Access Point – urządzenia do zbudowania w placówce sieci bezprzewodowej obejmującej wszystkie pomieszczenia.

Od urządzeń zastosowanych do budowy sieci teleinformatycznej wymagane będzie spełnienie następujących wymagań:

- Router
- Bezpieczeństwo aplikacji oraz danych zgromadzonych w systemie gwarantować będzie dedykowane urządzenie - router.

Planuje się by zastosowane urządzenie posiadało następujące funkcjonalności:

- wbudowana w router enkrypcja sprzętowa,
- obsługa co najmniej 1000 tuneli VPN,
- zapobieganie włamaniom Intrusion Prevention,
- zabezpieczenie antywirusowe poprzez mechanizmu Network Admission Control (NAC),
- pełna wydajność łącza (wire-speed) dla równoległego przesyłania danych, głosu,
- realizacja funkcji bezpieczeństwa oraz usług zaawansowanych dla łączy o przepustowości rzędu kilkukrotności łączy E1 (4-10 Mbps),
- porty (UTP) 10/100 BaseTx,
- obsługa przełączania L2,
- przesyłanie głosu - obsługa połączeń analogowych i cyfrowych,
- możliwość integracji usług, takich jak sprzętowa kompresja i szyfrowanie danych,
- obsługa funkcji związanych z poziomem jakości usług, takich jak: Resource Reservation Protocol (RSVP), Weighted Fair Queueing (WFQ), Class Based Weighted Fair Queueing (CBWFQ), Low Latency Queueing (LLQ) i IP Precedence,
- graficzny interfejs użytkownika,
- możliwość automatycznej konfiguracji poprzez sieć WAN,
- możliwość ustawienia w konfiguracji wieżowej z przełącznikami sieci LAN, w celu zapewnienia łatwiejszego administrowania.

Przełącznik Ethernet

Wskazane jest, aby były to urządzenia warstwy trzeciej. Pozwoli to na swobodę segmentacji logicznej sieci przy zachowaniu jej wysokiej wydajności. Umożliwi także implementację polityki łączenia, zarezerwowaną zwykle dla dedykowanej warstwy dystrybucji sieci. Ze

względu na różnorodność aplikacji wykorzystywanych w systemie, zalecane jest wykorzystanie urządzeń wspierających kolejkowanie pakietów z kilkoma poziomami jakości usług QoS.
W celu zapewnienia łatwości zarządzania urządzeniami sieciowymi zaleca się zastosowanie urządzeń od jednego producenta wraz z dedykowanym oprogramowaniem wspomagającym zarządzanie. W placówce planuje się zastosowanie przełączników Ethernet typu 10/100/1000BaseTX o minimum 24 portach.

Access Point

W celu realizacji idei pełnego osieciowania placówki, zdecydowano się na wybranie rozwiązania opartego o technologię bezprzewodową. Takie podejście do zagadnienia, da pełen dostęp do sieci w każdym miejscu placówki i uniezależni od dostępu do gniazda sieciowego dla ewentualnych przyszłych aplikacji.
Od Bezprzewodowego Punktu Dostępowego wymagać się będzie:

- pracy w standardach 802.11b/g (pasmo 2,4 GHz) i 802.11a (pasmo 5 GHz).
- prędkości transmisji 54 Mbps (dla IEEE 802.11g).
- obsługi minimum 16 sieci VLAN, co pozwoli na zróżnicowanie praw dostępu, usług, zasad korzystania, poziomu bezpieczeństwa i QoS oraz umożliwi bardziej efektywne wykorzystanie pasma i zwiększenie przepustowości sieci.
- wyposażenia w minimum jeden port LAN 10/100 Mb/s tak (1 szt.).
- obsługi szyfrowania z zastosowaniem: 64/128 bit WEP, AES, TKIP, WPA, WPA2 (PSK). - WiFi Protected Access 2 (Pre-Shared Keys), WPA (802.1x).

Ad.2 Serwery

Zakłada się, że środowisko przetwarzania danych będzie składało się z czterech serwerów:

- bazodanowego
- aplikacyjnego
- portalowego
- bezpieczeństwa i backupu danych

Planuje się, że rozwiązanie infrastruktury przetwarzania danych składało się będzie, z co najmniej czterech podobnie wyposażonych serwerów – najlepiej z jednej linii produktowej (ze względu na wymienność podzespołów) o odpowiedniej mocy przetwarzania wraz z przewidzianą rezerwą mocy do realizacji funkcji pomocniczych, związanych z zabezpieczeniem oraz archiwizacją na wymiennych nośnikach przetwarzanych w systemie

danych. Maszyny powinny być dołączone zwielokrotnionymi szybkimi interfejsami do sieci informatycznej, przez którą aplikacje będą udostępniane użytkownikom. Dane przetwarzane w systemie udostępniane powinny być serwerom ze wspólnej macierzy dyskowej o wysokiej wydajności (najlepiej FC lub min. SCSI Ultra320), podłączonej wielokrotnie do serwerów poprzez przełącznik sieci SAN.

Planuje się, że serwery powinny spełniać następujące minimalne warunki:

- Obudowa: do montażu w szafie rack wraz z szynami, redundantne wentylatory typu hot-plug.
- Zasilanie: redundantne, przynajmniej dwa zasilacze typu HotPlug o mocy minimum 1500W.
- Płyta główna: z możliwością zainstalowania czterech procesorów, szyna FSB min. 1066MHz.
- Zainstalowane procesory czterordzeniowe klasy x86 dedykowane do pracy w serwerach zaprojektowane do pracy w układach wieloprocesorowych, o częstotliwości szyny systemowej min 1066MHz, pamięci L2 8MB.
- Pamięć: minimum 64GB registered ECC DIMM, rozszerzalna do 128 GB, na płycie powinno się znajdować co najmniej 16 slotów na pamięć. Dostępne zabezpieczenia: DIMM sparing, Single Device Data Correction (SDDC), Mirroring.
- Zintegrowany kontroler: typu RAID, cache 256MB, podtrzymanie bateryjne cache; obsługa RAID 0, 1, 5,6, 10, 50, 60; Dyski: minimum 2x 146GB 15krpm hot plug w RAID1.
- Sieć: minimum 4x Ethernet 10/100/1000 oraz karty światłowodowe jednoportowe FC4.

Planuje się, że pamięć masowa powinna spełniać następujące minimalne warunki:

- Moduł podstawowy - do instalacji w standardowej szafie typu rack 19".
- Dwa kontrolery RAID pracujące w układzie active-active udostępniające minimum 4 porty FC na kontroler do podłączenia switchy lub serwerów. Wymagane poziomy RAID: 0,1,3,5,6,10; Cała macierz powinna umożliwiać rozbudowę interfejsów zewnętrznych przez umieszczenie w module podstawowym portów FC i portów iSCSI, Cache: z opcją przydziału przez administratora pamięci dla zapisu i odczytu; minimum 8GB sumarycznie, pamięć cache zapisu mirrorowana między kontrolerami, z opcją zapisu na dysk lub podtrzymywana bateryjnie przez min.48h w razie awarii.

- Dyski: typu Hot-Plug, najlepiej typu FC4 15x300GB 15krpm, możliwość rozbudowy przez dokładanie kolejnych dysków/półek dyskowych, bez przerywania pracy macierzy.
- Bezpieczeństwo pracy macierzy: brak pojedynczego punktu awarii, ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne, możliwość wymiany na gorąco bez zatrzymywania pracy macierzy.
- Oprogramowanie zarządzające macierzą: powiadamianie mailem o awarii, umożliwiające maskowanie i mapowanie dysków. Macierz powinna posiadać licencję umożliwiającą podłączenie do niej min. 256 hostów, licencję umożliwiającą rozbudowę macierzy do pełnej pojemności oraz powinna umożliwiać definicję min. 1024 dysków logicznych (LUN). Upgrade oprogramowania macierzy bez zatrzymywania pracy macierzy. Dostarczana macierz powinna być wyposażona w funkcjonalność wykonywania kopii pełnych i migawkowych, realizacji failover oraz load balancing na podłączeniach wielościeżkowych serwerów do macierzy dla wszystkich wspieranych systemów operacyjnych. Możliwość rozbudowania oprogramowania o funkcjonalność zdalnej synchronicznej i asynchronicznej replikacji danych poprzez wykorzystanie wbudowanych w macierz funkcji mirroringu synchronicznego i asynchroniczny. Mirroring danych musi być realizowany na poziomie mikrokodu macierzy.

Wymagane jest także dostarczenie kompletu kabli światłowodowych FC do redundantnego podłączenia infrastruktury SAN.

Przełącznik sieci SAN

- Obudowa: do instalacji w standardowej szafie typu rack 19",
- Porty: minimum 16 aktywnych portów FC, obsługiwane standardy: FL_Port, F_Port, E_Port, Class 2, Class 3, Class F. Możliwość rozbudowy/aktywowania kolejnych portów,
- Oprogramowanie: zarządzające switchami przez SNMP i WWW; monitorujące stan pracy. Wymagana licencja full fabric oraz funkcjonalność trunking'u.

Szafy rack:

Planuje się, że serwery oraz macierz powinny być zainstalowane w dwóch szafach typu rack, spełniających następujące wymagania:

- wysokość minimum 42U, głębokość minimum 100cm, przednie i tylne drzwi perforowane, zamykane na klucz, boczne ściany zdejmowane, minimum dwie półki, szafa powinna mieć możliwość łączenia z innymi szafami – tego samego typu/modelu.

- Konsola zarządzania: wyposażona w monitor wysuwany o wysokości 1U, minimum 17", klawiatura z urządzeniem wskazującym,
- Przełącznik iKVM 16-to portowy, z możliwością podłączenia serwerów zarówno z interfejsem USB jak i PS2, o funkcjonalności wyszukiwania podłączonych serwerów, możliwość nadawania nazw podłączonym serwerom, komplet kabli do podłączenia serwerów wyposażonych w interfejs USB. Razem z szafami powinny być dostarczone panele wypełniające w liczbie niezbędnej do wypełnienia pustych przestrzeni szaf.

Ze względu na bardzo szybki postęp techniczny w tym obszarze, szczegółowe parametry techniczne powinny zostać zaktualizowane i precyzyjnie określone w momencie ogłaszania postępowania na wybór wykonawcy.

Dla potrzeb niniejszego opracowania, do obliczeń przyjęto, że serwery to wysokowydajne komputery firmy Dell model R900, a macierz dyskowa to model Dell EMC Cxx.

Zakłada się, że system backupu będzie oparty o modularna bibliotekę taśmową oraz współpracujące z nim oprogramowanie wspomagające i automatyzujące proces backupu.

Zakłada się, że urządzenie do backupu danych będzie spełniać następujące warunki

1. Obudowa: przystosowana do instalacji w standardowej szafie typu rack 19".
2. Napędy: minimum 2 x LTO3 lub LTO4, najlepiej z możliwą dalszą rozbudową.
3. Liczba slotów: minimum 48 z możliwością dalszej rozbudowy.
4. Interfejsy: natywne FC napędów.
5. Interfejs do zarządzania poprzez przeglądarkę WWW oraz możliwość zarządzania bezpośrednio z użyciem wbudowanych klawiszy i wyświetlacza LCD, wsparcie dla zarządzania z wykorzystaniem SNMP.
6. Wsparcie dla nośników LTO WORM (Write Once, Read Many), umożliwiających spełnienie norm prawnych dotyczących odpowiednio długiego przechowywania nienaruszonych danych (archiwizacja).
7. Redundantne zasilacze hot-swap, napędy typu hot-swap.
8. Komplet kabli światłowodowych do podłączenia do sieci SAN.
9. Minimum 50 taśm wraz z kompletem etykiet oraz min 2 kasety czyszczące.

Oprogramowanie do backupu danych musi zapewnić tworzenie:

1. Kopii zapasowych plików i konfiguracji systemów operacyjnych dla wszystkich serwerów Zamawiającego.

2. Kopii zapasowych instalacji i podstawowego odtwarzania systemu (BMR) dla wszystkich serwerów Zamawiającego.
3. Kopii zapasowych Relacyjnej Bazy Danych dla serwera bazodanowego.

Dla celów obliczeniowych przyjęto rozwiązanie firmy Dell model PV ML6000 Tape Autoloader.

Ad. 3 Zestawy komputerowe typu PC.

Przedmiotem tej części projektu będzie dostawa 50 zestawów komputerowych typu PC składających się z:

1. Komputerów typu PC,
2. Urządzeń peryferyjnych - drukarek, skanerów i urządzeń wielofunkcyjnych.

Ze względu na bardzo szybkie zmiany zachodzące w konfiguracjach i parametrach tego typu sprzętu, niecelowym jest w tym miejscu określanie parametrów technicznych stanowisk użytkowników. Należy jedynie podkreślić by zamawiany sprzęt był fabrycznie nowy i cechował się na daną chwilę aktualnymi parametrami technicznymi. Szczegółowe parametry techniczne powinny zostać zaktualizowane i precyzyjnie określone w momencie ogłaszania postępowania na wybór Wykonawcy.

Drukarki – tak jak w przypadku sprzętu komputerowego, sprawę określenia parametrów technicznych należy odłożyć na moment rozpoczęcia wdrożenia. Należy pamiętać by zakupywane drukarki były wyposażone we własne interfejsy sieciowe oraz drukowały w technologii laserowej.

Alternatywnie rozważa się możliwość wyposażenia wszystkich placówek w terminale zamiast komputerów PC. Rozwiązanie to przy porównywalnym koszcie, dałoby olbrzymie korzyści w obszarze administrowania i utrzymania ciągłości pracy całego systemu. Jednak warunkiem decydującym o możliwości zastosowanie tego typu rozwiązania jest posiadanie odpowiedniej jakości (pod względem przepustowości i pewności działania) sieci WAN.

Planuje się, że decyzja o modelu dostarczanego sprzętu do placówek zostanie podjęta po rozstrzygnięciu postępowania na dostarczanie usług dostępu do Internetu.

Do obliczeń przyjęto, że stacje robocze to komputery firmy Dell model OptiPlex. Wysoką wydajność komputera zapewnia dwurdzeniowy procesor Intel Core 2 Duo pracujący z częstotliwością 2,8 GHz i zawierający 3 MB pamięci podręcznej L2. Komputer wyposażony jest w klawiaturę i mysz optyczną. Dodatkowo jego funkcjonalność podnosi wbudowana

nagrywarka DVD. Komfort pracy użytkownika powinien być zapewniony przez zastosowanie monitorów LCD o przekątnej 17".
Jako oprogramowanie systemowe stacji roboczych przyjęto system Microsoft Windows Vista PL w wersji Business.

Ad. 4 Telefonia VoIP

Wykorzystanie technologii cyfrowej w transmisji danych umożliwia przesyłanie dźwięku na dowolne odległości bez strat przesyłowych. Połączenie globalnego zasięgu Internetu oraz wysokiej jakości cyfrowej transmisji głosu umożliwiło opracowanie alternatywy dla dotychczasowych rozwiązań telefonii analogowej: telefonii VoIP (ang. Voice over Internet Protocol).
W telefonii VoIP przesyłanie głosu odbywa się w postaci cyfrowej poprzez sieci rozległe WAN. W pierwszej fazie transmisji następuje zamiana głosu na postać cyfrową, poddanie go procesowi kompresji i podzielenie na mniejsze pakiety. Każdy z pakietów przebywa drogę od nadawcy do docelowego odbiorcy w sposób niezależny. Droga porcji głosu wybierana jest przez urządzenia w sieci w oparciu o adresy IP, źródła głosu i miejsce przeznaczenia. Przesyłany strumień pakietów jest transportowany wraz z innymi danymi pochodzącymi na przykład z komputerów (współdzielenie pasma transmisji).
W punkcie odbiorczym cały proces kompresji i podziału głosu odtwarzany jest w odwrotnym kierunku, dzięki czemu otrzymujemy sygnał głosowy. Cyfrowa transmisja przesyłanego głosu wyklucza pojawianie się szumów i zniekształceń. Momenty ciszy nie są przesyłane. Taki model transmisji znaczne usprawnia i zmniejsza obciążenie procesu przesyłu danych.
Przewagami tej technologii są znacznie niższe koszty eksploatacji, wyższa jakość przekazu głosowego oraz większa funkcjonalność stosowanych urządzeń i usług. Obecnie dzięki powszechnemu dostępowi do Internetu systemy opierające się o usługę VoIP stają się coraz bardziej popularne i częściej stosowane.

Funkcjonalność

Zakładane do realizacji w ramach niniejszego projektu rozwiązanie umożliwia płynne przejście od tradycyjnej sieci telefonicznej do sieci opartej o transmisję VoIP. Płynne przejście oznacza zarówno zachowanie istniejącej topologii komunikacyjnej, jak również ochronę dokonanych wcześniej inwestycji. System telefonii VoIP będzie komunikować się z publiczną siecią telefoniczną poprzez urządzenie dostępowe i centralę telefoniczną Urzędu Miasta Łodzi.

Komunikacja pomiędzy wszystkimi placówkami Beneficjenta oraz samym Urzędem będzie mogła odbywać się wyłącznie w oparciu o technologię VoIP.

Podstawowe funkcjonalności realizowane przez platformę telefonii VoIP to:

- Centralne sterowanie z możliwością rozproszenia zasobów.
- Duża pojemność i wydajność systemu telefonicznego.
- Elastyczność systemu (łatwość modelowania systemu, lokalizacji, styku z siecią PSTN).
- Bezpieczeństwo przesyłanej informacji.
- Szeroka gama telefonów działających w oparciu o standard SIP.
- Możliwość stosowania telefonów działających w technologii bezprzewodowej.
- Bardzo proste zestawianie i obsługa połączeń video (zestawienie rozmowy video, jest tak samo proste jak zestawienie klasycznego połączenia telefonicznego).
- Usługi dodane (aplikacje XML, uruchamiane na ekranach telefonów IP: kalendarze, informator, itp.).
- Obsługa pracowników zdalnych – użytkownik rejestruje swój softphone poprzez sieć VPN.
- Śledzenie stanu obecności/linii innych użytkowników.
- Połączenia głosowe z dowolnym użytkownikiem telefonii konwencjonalnej, cyfrowej, satelitarnej, komórkowej i internetowej na całym świecie.
- Połączenia konferencyjne.
- Obsługa połączeń oczekujących.
- Prezentacja numeru dzwoniącego (CLIP).
- Blokada prezentacji własnego numeru (CLIR).
- Blokowanie połączeń na wybrane numery.
- Obsługa numerów wewnętrznych.
- Przekazywanie połączeń na wybrany numer.
- Przekierowanie połączeń z zajętych numerów.
- Poczta głosowa – Voice2Email.
- Możliwość preferowania/blokowania określonych połączeń przychodzących.
- Biling dostępny on-line przez stronę WWW.
- Obsługa faksu - Fax2Email; Email2Fax.
- Wielopoziomowa obsługa standardowych komunikatów głosowych – IVR.

Opis podstawowych funkcjonalności systemu telefonii IP

Telefony IP oferują całą gamę funkcjonalności telefonicznych dostępnych w systemach klasycznych PBX. Dodatkowo z racji wykorzystania technologii IP, telefony zyskują nowe,

dotychczas niemożliwe do zrealizowania funkcje. Poniżej przedstawiono krótki opis podstawowych funkcji dostępnych dla telefonów IP.

Identyfikacja połączeń telefonicznych

Jak w każdym dużym klasycznym systemie telefonicznym, także w rozwiązaniu telefonii IP możliwa jest pełna identyfikacja połączeń telefonicznych, zarówno przychodzących, jak też i wychodzących. Dla połączeń wewnętrznych (tj. zestawianych pomiędzy dwoma telefonami IP) przekazywany jest numer dzwoniącego, a także jego nazwa (o ile została skonfigurowana przez administratora). Dla połączeń zewnętrznych, tzn. wychodzących z systemu telefonii IP do publicznej sieci telefonicznej (oraz dla połączeń przychodzących – w odwrotnym kierunku) przekazywana jest identyfikacja numeru dzwoniącego, o ile tylko zastosowany typ styku do sieci publicznej to umożliwia. Aby to uzyskać, rekomendowane jest stosowanie styków z sygnalizacją ISDN Q.931 (np. ISDN BRA lub ISDN PRA).

System telefonii IP umożliwia także niemal dowolne manipulowanie numerami – np. w taki sposób, aby do jednych użytkowników identyfikacja wyglądała na skróconą (np. trzy cyfry numeru wewnętrznego), a dla innych na pełną (np. pełen siedmio- lub dziewięcio-cyfrowy numer zgodny z publicznymi numerami telefonicznymi). Ponadto, administrator ma możliwość zablokowania prezentacji numeru dla wybranych linii lub połączeń. W systemie telefonii IP identyfikacja (zarówno po numerze, jak też i po nazwie) ma zawsze charakter centralny, jako że to elementy kontrolno-sterujące tego systemu przekazują za pomocą odpowiednich protokołów sygnalizacyjnych wszelkie informacje do i z telefonów IP.

Przenoszenie i przekierowywanie połączeń telefonicznych

W systemie telefonii IP, podobnie jak w każdym dużym, klasycznym systemie telefonicznym, możliwe jest elastyczne przenoszenie (tzw. *transfer*) już odebranych połączeń oraz przekierowywanie (czyli tzw. *forwarding*) połączeń, które dopiero mają nadejść.

Użytkownik telefonu IP może zrealizować tzw. bezwarunkowe przeniesienie rozmowy (czasami nazywane „przeniesieniem w ciemno"), jak też i wykonać przeniesienie dopiero wtedy, gdy osoba, do której ma nastąpić przekazanie rozmowy, odbierze połączenie i zgodzi się na jego przyjęcie (operacja ta zwana jest czasami „przeniesieniem z konsultacją"). W przypadku przeniesienia połączenia, abonent do którego zostało ono przekazane, będzie widział na wyświetlaczu swojego telefonu informację o dzwoniącym taką samą, jak osoba, która początkowo odebrała to połączenie. Przekierowywanie połączeń realizowane jest w systemie telefonii IP podobnie jak w systemach telefonii klasycznej. Możliwe jest

skonfigurowanie bezwarunkowego przekierowania (wszystkie połączenia), przekierowania przy braku odpowiedzi oraz w przypadku zajętości linii. Użytkownik telefonu IP może podobnie jak użytkownik telefonu klasycznego skonfigurować przekierowanie bezwarunkowe bezpośrednio na telefonie podając numer, na który mają być kierowane połączenia. Jednakże w odróżnieniu od telefonii klasycznej, użytkownik ma także możliwość zmiany sposobu przekierowania połączeń poprzez webowy interfejs graficzny. Istnieje także możliwość „łańcuchowej" konfiguracji przekierowania połączenia. Domyślnie system telefonii IP dopuszcza do 12 poziomów „zagnieżdżeń" przekierowania rozmowy, choć wartość tego parametru administrator może zmienić wedle własnego uznania.

Zawieszanie rozmowy

W systemie telefonii IP, możliwe jest chwilowe zawieszanie prowadzonej rozmowy (tzw. *Hold*). W trakcie, gdy rozmowa jest zawieszona, użytkownik telefonu IP może przyjąć lub samemu wykonać inne połączenie telefoniczne. Jednocześnie w tym czasie, w zależności od konfiguracji systemu, rozmówca, z którym rozmowa została zawieszona, słyszy w swojej słuchawce odpowiednią muzykę „oczekiwania" (tzw. *music-on-hold*). W odróżnieniu od klasycznych systemów telefonicznych, w telefonii IP sygnał music-on-hold może być wybierany indywidualnie dla każdego urządzenia, a ponadto pochodzi on z plików zapisanych w standardowym formacie WAV. Dzięki temu można uzyskać np. taką konfigurację, w której w przypadku połączenia przychodzącego z zewnątrz, które jest przez użytkownika telefonii IP zawieszane, odgrywana jest zwykła muzyka, jednakże w przypadku połączeń wewnętrznych do wybranych np. do helpdesku, w przypadku zawieszenia rozmowy odgrywane są komunikaty o bieżących problemach w działaniu struktury informatycznej.

Ponadto oprócz typowej funkcji zawieszenia rozmowy, użytkownicy telefonii IP mają także możliwość wykonania operacji przeniesienia rozmowy na tzw. parking. Pozwala to następnie wznowić tą rozmowę w dowolnej chwili z zupełnie innego aparatu.

Telekonferencje

Obsługa telekonferencji jest standardową cechą funkcjonalną systemu telefonii IP. Użytkownik prowadzący rozmowę telefoniczną może w dowolnej chwili zażądać od systemu włączenia do niej kolejnych uczestników. Użytkownik zestawiający w trybie „na żądanie" (nazywanym także trybem „ad-hoc") takie połączenie telekonferencyjne ma w każdej chwili możliwość usunięcia z niego ostatniego dodanego uczestnika. Jest to bardzo ważna funkcja, która staje się wręcz niezbędna np. w przypadku, gdy zamiast połączenia się z użytkownikiem, którego

chcemy włączyć do telekonferencji (a który jest nieobecny lub po prostu nie odbiera połączenia), zostaje przyłączona do niej jego skrzynka poczty głosowej.
Ponadto, oprócz telekonferencji zestawianych „ad-hoc", użytkownicy systemu telefonii IP mają możliwość wcześniejszego aranżowania takich połączeń – wtedy wszyscy zaproszeni do niej użytkownicy o określonej godzinie łączą się z podanym im uprzednio numerem. W zależności od konfiguracji sprzętowej systemu telefonii IP, w konferencji aranżowanej może uczestniczyć od 6-ciu do nawet kilkuset użytkowników telefonii IP.

Wideokonferencje

System telefonii VoIP daje również unikalne możliwości w zakresie rozmów wideo. Telefon IP współpracuje z komputerem osobistym użytkownika oraz dedykowanym oprogramowaniem (Video Advantage) oraz kamerą USB (VT II). W przypadku rozmowy wideokonferncje zestawiane są „przy okazji" zwykłego połączenia telefonicznego. Daje to możliwość dołączania użytkowników do wideo-konferencji (jeżeli istnieje mostek) np. w trybie meet-me.
W przypadku wideokonferncji niezbędne jest zastosowanie zasobu sprzętowego (mostka wideo) pozwalającego na realizację wideokoferencji. W ofercie firmy Cisco System znajdują się rozwiązania z serii IPVC 35xx mogące łączyć w jednej konferencji terminale H.323,SCPP oraz SIP. Dostępne są różne modele mostków, różniące się parametrami oraz wydajnością

Intercom

Funkcja ta może działać w dwóch trybach: Intercom i Whisper. Tryb Intercom to możliwość strumieniowania treści audio do określonej grupy osób. Tryb Whisper aktywowany jest w przypadku, gdy osoba do której strumieniowany jest przekaz rozmawia z innym abonentem (tryb dyskretny). Przekaz słyszalny jest tylko w słuchawce odbiorcy.

Do Not Disturb

Telefonia VoIP daje możliwość pracy telefonu w trybie (DnD –Do Not Disturb). Telefon w tym trybie nie sygnalizuje przychodzącego połączenia dzwonkiem. Na telefonie widnieje komunikat o „cichym" trybie pracy. Połączenie przychodzące może być jednak sygnalizowane w tym trybie poprzez:

- Beep
- „Błyśnięcie" lampki telefonu
- Bez sygnalizacji

Programowalne klawisze liniowe (tylko telefony SCCP)

W niektórych wersjach systemu istnieje możliwość programowania klawiszy liniowych, tak aby spełniały następujące nowe funkcje (np. Hold, CallBack, Forward All, Park, itp.). Ustawienia te są nadawane i programowane przez administratora systemu. Użytkownik końcowy nie może zmienić tych ustawień.

Opis funkcjonalny modułu Contact Center

Jednym z podstawowych elementów „Łódzkiego Centrum Kontaktu z Mieszkańcami" będzie Contact Center – rozwiązanie zapewniające telefoniczną łączność interesantów z operatorami ŁCKM. Proponowane rozwiązanie techniczne powinno być elastyczne, skalowalne i oparte o technologię IP, co w przypadku aktualnej infrastruktury Urzędu zapewnia łatwą implementację i późniejszy rozwój systemu. Zaimplementowany system powinien mieć możliwość łatwej rozbudowy systemu do modelu rozproszonego, dodawania kolejnych agentów, zmiany ich umiejętności, rozbudowy systemu automatycznego IVR i multimedialnego centrum kontaktowego AIC. System powinien być zaprojektowany w taki sposób, aby zapewnił bezproblemową 24-ro godzinną pracę ŁCKM.

Podstawowe wymagania funkcjonalne :

1. System powinien umożliwiać klientowi kontakt z „Łódzkim Centrum Kontaktu z Mieszkańcami" z wykorzystaniem następujących kanałów telekomunikacyjnych: Telefon, Fax, E-mail, Chat, WWW.
2. System powinien umożliwiać obsługę mieszkańca z udziałem pracownika „Łódzkiego Centrum Kontaktu z Mieszkańcami" z inicjatywy mieszkańca lub pracownika „Łódzkiego Centrum Kontaktu z Mieszkańcami" oraz poprzez system samoobsługowy telefonicznych interaktywnych odpowiedzi głosowych.
3. System powinien zawierać moduły: IVR (Automatyczny System Informacyjny), PBX (Private Branch Exchange), ACD (Automatyczna Dystrybucja Rozmów), obsługi: poczty elektronicznej, faksów, kampanii wychodzących - outbound (poprzez e-mail, fax, głos).
4. System powinien umożliwiać rozliczanie połączeń telefonicznych, rejestrację rozmów telefonicznych, analizy i raportowania pracy systemu, efektywne wykorzystywanie narzędzi diagnostyki, administracji, konfiguracji systemu, tworzenia skryptów itp.
5. System powinien zapewniać pełną identyfikację i autentykację użytkowników oraz być wyposażony w zabezpieczenia przed niepowołanym dostępem.

6. System powinien być wyposażony w narzędzia nagrywania połączeń i rozmów oraz archiwizacji nagrań i ich odszukiwania.
7. System powinien zapewnić funkcjonowanie przez 24 h / 365 dni w roku.
8. System powinien umożliwiać obsługę klientów w liczbie 700 tys. z możliwością dalszej rozbudowy.
9. System powinien umożliwiać łatwą rozbudowę o dodatkowe centra zdalnej obsługi, podrzędne w stosunku do pierwotnej instancji systemu. Dodatkowe centra obsługi powinny mieć pełną możliwość współpracy z systemem podstawowym, przejmować w razie potrzeby część lub całość zadań związanych ze zdalną obsługą i stanowić dla siebie system rezerwowy na wypadek awarii.

Dalszą analizę techniczną przeprowadzono w oparciu o jedno z najpowszechniej stosowanych rozwiązań na polskim rynku call center – technologię i rozwiązania firmy AVAYA. Z oczywistych względów nie przesądza to o zastosowaniu tej technologii – wybór zostanie dokonany po przeprowadzeniu postępowania przetargowego.

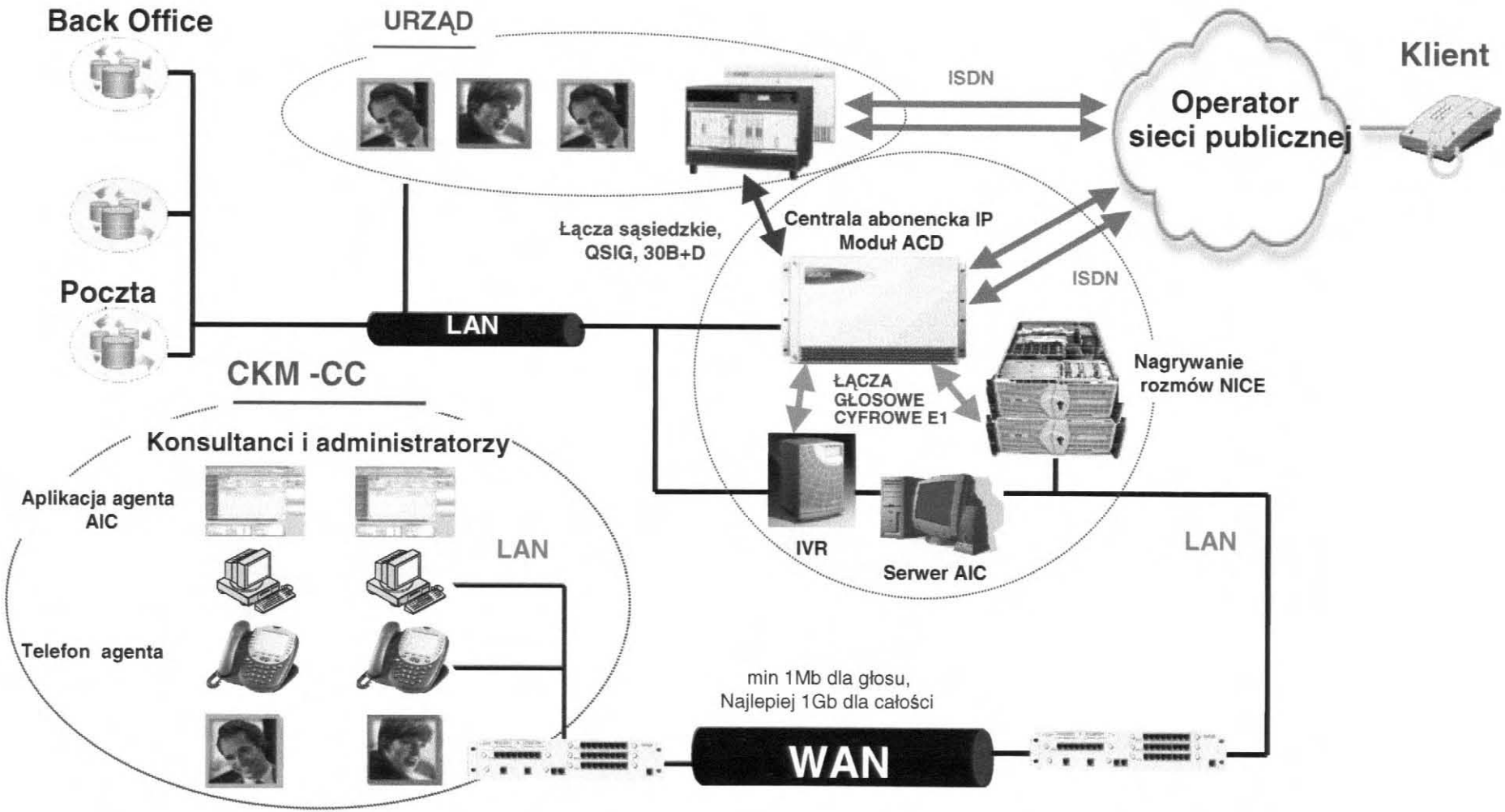
W związku z postawionymi powyżej warunkami funkcjonalnymi przewiduje się, że system teleinformatyczny zostanie wyposażony w co najmniej 25 licencji pakietu Call Center ELITE w centrali PBX-IP (składającej się z serwera i Media Gateway'a), 50 licencji głosowych na agentów i 10 licencji dla kanałów e-mail i faks w systemie CTI-Contact Center AIC. Współpracujący system obsługi automatycznej - IVR obejmie obsługę 30-u portów cyfrowych z możliwością ich szybkiej rozbudowy, poprzez dołożenie kart 30-to portowych i odpowiednich licencji. System samoobsługowy IVR jest częścią całej struktury multimedialnego Centrum Zgłoszeniowego. Przewiduje się, że wraz z podstawowymi komponentami systemu, dostarczony zostanie także system nagrywania połączeń NICE, pozwalający na nagrywanie dowolnego Agenta systemu, przechowywanie i archiwizowanie nagrań i ich odtwarzanie wg. określonych parametrów.

Planuje się, że proponowane rozwiązanie obejmie trzy warstwy:

- **Pierwsza warstwa** - infrastruktura komunikacji głosowej i internetowej z systemami PBX-IP, ACD, IVR i systemem nagrywania rozmów NICE.
- **Druga warstwa** - rozwiązanie Avaya Interaction Center (AIC) – będące aplikacją CTI (Computer Telephony Integration), scalającą w jednym środowisku wszystkie wpływające do i wychodzące kontakty multimedialne i pozwalająca na uruchamianie wewnątrz niej aplikacji biznesowej, na której będą pracować konsultanci ŁCKM.

- **Trzecia warstwa** - oprogramowanie użytkowe - aplikacje biznesowe (eBusiness Applications - Front End), zapewniające realizację wymaganych funkcji w zakresie współpracy z Agentami oraz oprogramowanie pośredniczące, służące do integracji z systemami „back-office".

Ogólny schemat systemu



Pierwsza warstwa tworzy interfejs telekomunikacyjny do obsługi kontaktów z klientami w ruchu przychodzącym i wychodzącym, np. za pomocą połączeń telefonicznych lub Internetu (e-mail). Elementy składające się na tę warstwę (PBX-IP, IVR, ACD, NICE, telefony) są połączone z oprogramowaniem AIC w drugiej warstwie z jednej strony, z drugiej strony z operatorami publicznymi bądź innymi centralami PBX za pomocą łączy sąsiedzkich.
Połączenie (kontakt) wchodzące do CC jest przekazywane do warstwy drugiej, do systemu Avaya Interaction Center, który rozdziela je do konkretnych agentów/konsultantów wg. inteligentnego algorytmu, wywołując na ekranach komputerów agentów odpowiednie okno aplikacji biznesowej (warstwa trzecia).
Informacje (np. usługa żądana w systemie IVR) zgromadzone w systemie TIP, mogą być po identyfikacji klienta przekazane do aplikacji biznesowej wypełniając odpowiednie jej pola.
Wszystkie operacje wykonywane w systemie Avaya Interaction Center są rejestrowane w systemie raportującymi „Operational Analyst". Administratorzy systemu CZ mogą w nim znaleźć przydatne informacje dotyczące pracy centrum kontaktowego, w zakresie wpływających kontaktów i efektywności pracy Agentów.

Opis architektury systemu

System Avaya Interaction Center wraz z systemami ACD i IVR będzie obsługiwać „Łódzkie Centrum Kontaktu z Mieszkańcami". Serwer główny AIC (warstwa 2) będzie realizował wszystkie podstawowe warianty obsługi różnych form interakcji z klientem. Serwer ten zapewni również funkcjonalność CTI oraz zarządzanie pocztą elektroniczną i kanałem faksowym. ACD, IVR oraz wszystkie pozostałe elementy składowe systemu Contact Center są płynnie zintegrowane. Serwer faksowy (nie będący częścią systemu) będzie zintegrowany za pomocą łącza poczty elektronicznej AIC z zastosowaniem protokołów POP3 i SMTP. Faksy będą obsługiwane jako załączniki e-mail w poczcie elektronicznej.
System Avaya Interaction Center jest multimedialnym rozwiązaniem centrum kontaktowego, na które składają się aplikacje, umożliwiające Łódzkiemu Centrum Kontaktu z Mieszkańcami zarządzanie informacjami. System AIC zapewnia uzyskanie jednolitego obrazu urzędu, jednolitego zestawu reguł spójności i przepływu czynności oraz jednolitego interfejsu Agentów w wszystkich mediach.

Opis funkcjonalny proponowanego rozwiązania

Zaproponowany system telekomunikacyjny PABX-IP/ACD będzie wykorzystywany do obsługi głosowego kanału kontaktu w projektowanym „Łódzkim Centrum Kontaktu