CELAB

Opis techniczny programu

Spis treści

1. Zadania systemu CELAB....2
2. Minimalne wymagania systemu CELAB....2
2.1. Stacja robocza....2
2.2. Serwer....2
2.3. Komputer do zabezpieczenia sieci....2
2.4. Łącze internetowe....3
2.5. Dodatkowe oprogramowanie....3
2.6. Czytniki....3
3. Architektura systemu....3
3.1. Moduł centralnej bazy danych - CELAB CBD....4
3.1.1. Baza danych SQL....5
3.1.2. Serwer aplikacji JBoss....5
3.1.3. Przeglądarka internetowa....6
3.2. Moduł obsługi laboratorium - CELAB LIMS....6
3.3. Szczegółowy schemat architektury systemu....7
3.4. Moduł statystyczny....9
4. Platforma programowo-sprzętowa....9
5. Bezpieczeństwo....9
5.1. IPSec....9
5.2. Open VPN....10
5.3. SSL....10
5.4. Hasła....10
5.5. Uprawnienia, kontrola dostępu....10
5.6. Zabezpieczenie sieci wewnętrznej (tzw. firewall)....11
5.7. Bezpieczny i szybki dostęp do stron WWW....11
6. Technologie programistyczne....11
6.1. Biblioteki FINN....11
6.2. J2EE....11
6.3. JSP....11
6.4. PowerBuilder....12
7. Wymiana danych....12
7.1. Współpraca z innymi systemami....12
7.2. Współpraca na poziomie aplikacji CBD....13
7.3. Współpraca na poziomie aplikacji LIMS....13
7.4. Wymiana danych między modułami systemu CELAB....14
7.5. Wydruki i raporty....16
8. Struktura bazy danych....16
9. Pozostałe rozwiązania informatyczne....17
9.1. Rejestracja czasu pracy....17
9.2. Podpis cyfrowy....18
10. Słowniki....18

1. Zadania systemu CELAB

Celem zintegrowanego systemu informatycznego CELAB jest usprawnienie pracy weterynaryjnych laboratoriów diagnostycznych oraz gromadzenie, przetwarzanie i publikacja danych o wynikach badań laboratoryjnych. System zapewnia pełną i efektywną kontrolę nad funkcjonowaniem ogólnopolskiej inspekcji weterynaryjnej, dostarcza rzetelnych informacji statystycznych na temat badań prowadzonych w laboratoriach oraz udostępnia dane dotyczące wyników dla uprawnionych organów, instytucji i jednostek badawczych.

2. Minimalne wymagania systemu CELAB

2.1. Stacja robocza

Procesor:	procesor Pentium II 350 MHz lub zgodny (zalecane: 1 GHz lub więcej)
Pamięć:	128 MB pamięci RAM (zalecane: 256 MB lub więcej)
Karta graficzna:	rozdzielczość 800x600 (zalecane: 1024x768 lub więcej)
Monitor:	CRT kolorowy 15" (zalecane: 17")
System operacyjny:	Windows 98 (zalecany: Windows XP) lub Linux z kernelem 2.6 (zalecany: Fedora Core 4)

2.2. Serwer

Procesor:	procesor Xeon 2,8 GHz
Płyta główna:	FSB 800 MHz
Pamięć:	1 GB
Dysk twardy:	40 GB
Karta sieciowa:	Ethernet 100 Mbps
System operacyjny:	PLD Linux z kernelem 2.6 (lub zgodny)

2.3. Komputer do zabezpieczenia sieci

Procesor:	procesor klasy Pentium II 350MHz lub Celeron 400MHz
Pamięć:	64 MB pamięci RAM
System operacyjny:	PLD Linux z kernelem 2.6 (lub zgodny)

2.4. Łącze internetowe

Przepustowość:	512 kb/s do użytkownika i 256 kb/s od użytkownika
Publiczny i stały adres IP:	TAK (Warunkowo możliwa jest praca zdalna w przeglądarce z lokalizacji bez tzw. stałego adresu IP. Będzie się to wiązało z ograniczeniem pełnej funkcjonalności systemu i obniżeniem bezpieczeństwa pracy.)

2.5. Dodatkowe oprogramowanie

Przeglądarka internetowa:	Internet Explorer 6.0 lub nowszy Mozilla Firefox 1.5 lub nowszy (zalecana)
Przeglądarka plików PDF:	Adobe Reader 7.0 lub nowszy

2.6. Czytniki

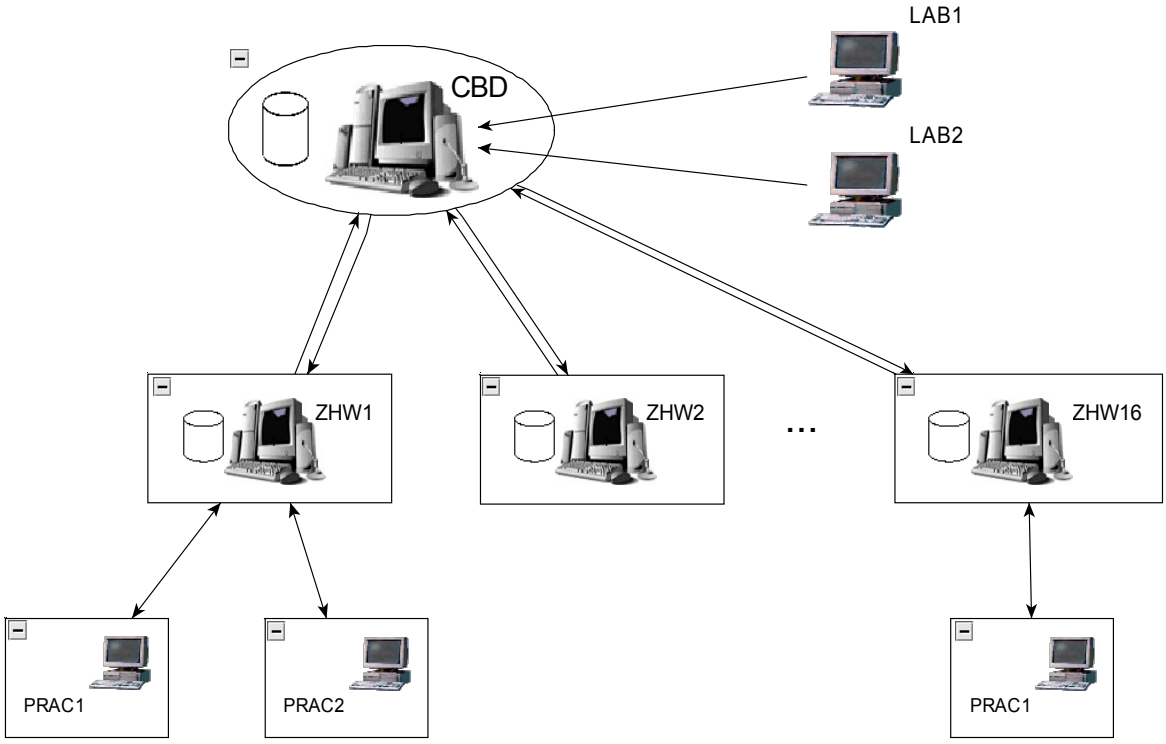
Rejestrator czasu pracy:	Tango I firmy Control System FMN
Czytnik kodów paskowych:	Podłączany przez złącze klawiatury

3. Architektura systemu

System CELAB w naturalny sposób dzieli się na dwa niezależne moduły - moduł centralnej bazy danych oraz moduł obsługi laboratoriów ZHW.

W ramach podstawowych ustaleń dotyczących architektury systemu zdecydowano o jednoznacznym wyróżnieniu 16-tu jednostek odpowiadających wojewódzkim ZHW, w których zainstalowano lokalne, niezależne bazy danych oraz samodzielne systemy serwerowe z aplikacją CELAB. Wszystkie zewnętrzne pracownie pracują w aplikacji przez Internet, bezpośrednio korzystając z lokalnej bazy danych ZHW.

Ogólną koncepcję przedstawia poniższy schemat:



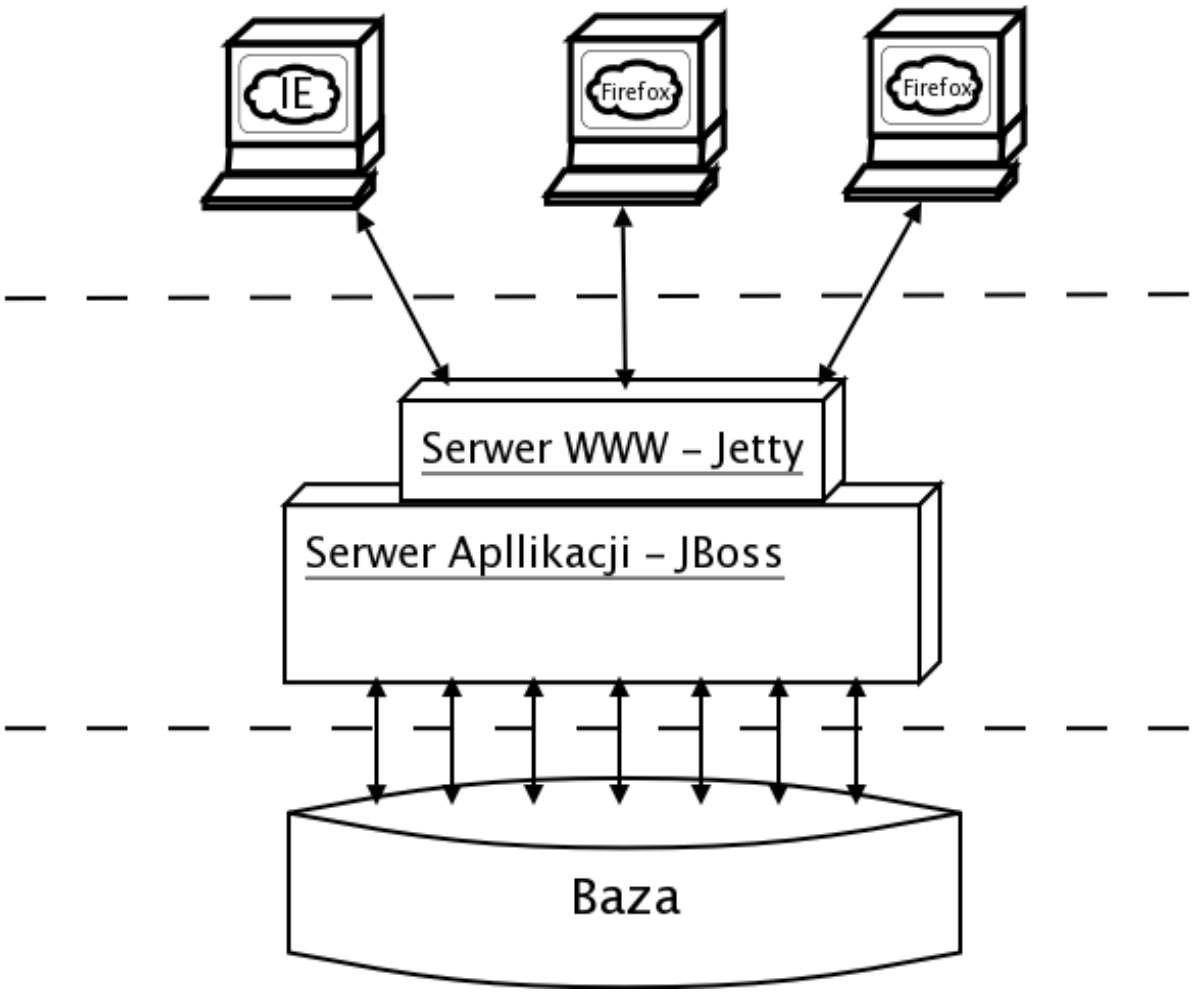
3.1. Moduł centralnej bazy danych - CELAB CBD

Moduł CELAB CBD jest pod względem technicznym w dużej części niezależny od pozostałych elementów systemu.

Moduł CBD obejmuje następujące zadania i funkcje:

- Gromadzenie i przechowywanie wszystkich danych globalnych wykorzystywanych przez wszystkie pozostałe elementy systemu (słowniki globalne, kartoteki).
- Gromadzenie i przechowywanie danych przesyłanych z poszczególnych laboratoriów.
- Gromadzenie i przechowywanie danych na temat planów badań monitoringowych i ich realizacji.
- Udostępnienie przez aplikację internetową zgromadzonych danych uprawnionym jednostkom.
- Sporządzanie raportów i zestawień na potrzeby odpowiednich organów.
- Sporządzenie raportów statystycznych.
- Kontrola poprawności i spójności danych.
- Automatyczna wymiana danych z oprogramowaniem CELAB do obsługi laboratoriów ZHW.
- Wymiana danych poprzez importy i eksporty z innymi systemami informatycznymi.
- Zabezpieczenie danych przed nieuprawnionym dostępem i kontrola uprawnień.
- Zarządzanie użytkownikami systemu CBD i nadawanie praw dostępu.
- Automatyczna archiwizacja danych i tworzenie kopii zabezpieczających.
- Automatyczne, okresowe generowanie tabel zawierających zagregowane metadane do złożonych raportów (patrz rozdział 7.5. Wydruki i raporty).

System CBD został napisany jako aplikacja w architekturze trójwarstwowej.



3.1.1. Baza danych SQL

Do realizacji projektu został wykorzystany system PostgreSQL. Baza danych PostgreSQL jest oparta na otwartej licencji BSD. Jest bezpłatna do wszystkich zastosowań komercyjnych jak i niekomercyjnych, udostępniana wraz z pełnym kodem źródłowym, co zapewnia najlepszą możliwość dopasowania bazy do indywidualnych potrzeb. Jest to także zasadniczy czynnik szybkiego i skutecznego naprawiania błędów programu. Baza danych PostgreSQL dzięki licencji Open Source działa na wielu różnych platformach systemowych i sprzętowych. Dokładnie przetestowaną platformą systemową jest PLD Linux. Serwer bazy danych może jednak być posadowiony na dowolnym systemie Unixowym, a także na serwerze Windows NT/2000/XP. Standardową platformą sprzętową jest architektura x86 (Intel, AMD). Baza danych może jednak działać na większości platform, na których można zainstalować system Linux - na przykład na procesorach PowerPC.

PostgreSQL należy do najbardziej zaawansowanych systemów bazodanowych typu Open Source. Posiada duże możliwości funkcjonalne oraz charakteryzuje się stabilną pracą w środowisku Linux. Możliwościami nie ustępuje większości „dużych" rozwiązań komercyjnych. Podczas realizacji projektu zostały wykorzystane zaawansowane możliwości serwera takie jak procedury wbudowane, funkcje bazodanowe, tzw. triggery oraz zaawansowane elementy kontroli spójności informacji (klucze obce, klucze alternatywne, klucze unikalne, kontrola ograniczeń).

3.1.2. Serwer aplikacji JBoss

Serwer aplikacji JBoss jest oprogramowaniem typu Open Source. Jest dostępny bezpłatnie do wszystkich zastosowań komercyjnych i niekomercyjnych. Pełny kod źródłowy zapewnia także możliwość dopasowania serwera do indywidualnych potrzeb. Serwer JBoss implementuje standard J2EE (Java 2 Enterprise Edition) i stał się środowiskiem działania aplikacji systemu CELAB napisanych w języku Java firmy Sun. Dzięki wykorzystaniu sprawdzonych i dobrze przetestowanych

rozwiązań wybór platformy J2EE zapewnił optymalną wydajność oraz skalowalność systemu.

CELAB CBD, stanowiący centralny element systemu, został napisany w języku Java i jest aplikacją platformy J2EE. Został posadowiony na serwerze aplikacji JBoss w Państwowym Instytucie Weterynarii w Puławach. Podstawowa część systemu CELAB LIMS została napisana w języku Java (standard J2EE) i została posadowiona na serwerze aplikacji JBoss w 16-tu ZHW.

Wykorzystanie języka Java i technologii J2EE pozwala na korzystanie z bardzo bogatej standardowej biblioteki rozwiązań przeznaczonych na potrzeby aplikacji typu Enterprise, standardowej i niezależnej metody dostępu do bazy danych oraz obsługi nowoczesnych interfejsów wymiany danych opartych o XML.

3.1.3. Przeglądarka internetowa.

Dostęp do systemu CBD zapewnia interfejs aplikacji typu web, to znaczy że podstawowym oprogramowaniem klienckim jest standardowa przeglądarka internetowa. Ze względu na kwestie bezpieczeństwa, ale także ze względu na poziom obsługi standardów internetowych W3C, podstawowym programem zalecanym do pracy z CELAB CBD jest przeglądarka internetowa Mozilla Firefox (system będzie także poprawnie pracował w powszechnie wykorzystywanej przeglądarce Microsoft Internet Explorer 6).

Dostęp do aplikacji CBD można uzyskać po wprowadzeniu określonego adresu URL, a następnie po wprowadzeniu odpowiedniej nazwy użytkownika i hasła. Przejrzysty interfejs aplikacji oraz proste i wygodne metody pracy z aplikacją gwarantują wydajną pracę z systemem nawet dla użytkowników nieobeznanych z technologiami internetowymi.

Całość komunikacji z aplikacją CBD przebiega po szyfrowanym połączeniu SSL (Secure Sockets Layer) przy użyciu bezpiecznego klucza o długości 128 bitów.

3.2. Moduł obsługi laboratorium - CELAB LIMS

System obsługi laboratoriów ZHW jest z założenia systemem realizującym bardzo wiele różnych funkcji, których specyfika pozwala dokonać rozdziału na część związaną z przeprowadzaniem badań laboratoryjnych, gromadzeniem i przetwarzaniem ich wyników (w tym również przekazywaniem wyników do bazy centralnej) oraz na część związaną z zarządzaniem pracą laboratorium. Koncepcję podziału zadań przedstawiono w poniższej tabeli:

Badania laboratoryjne	**Zarządzanie laboratorium**
- rejestracja zleceń	- zarządzenie wyposażeniem
- rejestracja próbek	- zarządzanie bazą producentów
- rejestracja wyników badań	- zarządzanie materiałami w pracowniach
- sprawozdania z badań	- pożywkarnia
- przekazywanie wyników do bazy centralnej	- gospodarka magazynowa
- obsługa słowników lokalnych	- cenniki
- aktualizacja słowników globalnych	- fakturowanie
- obsługa urządzeń laboratoryjnych	- rozliczenia
	- sprzedaż, rozrachunki
	- kasa, bank

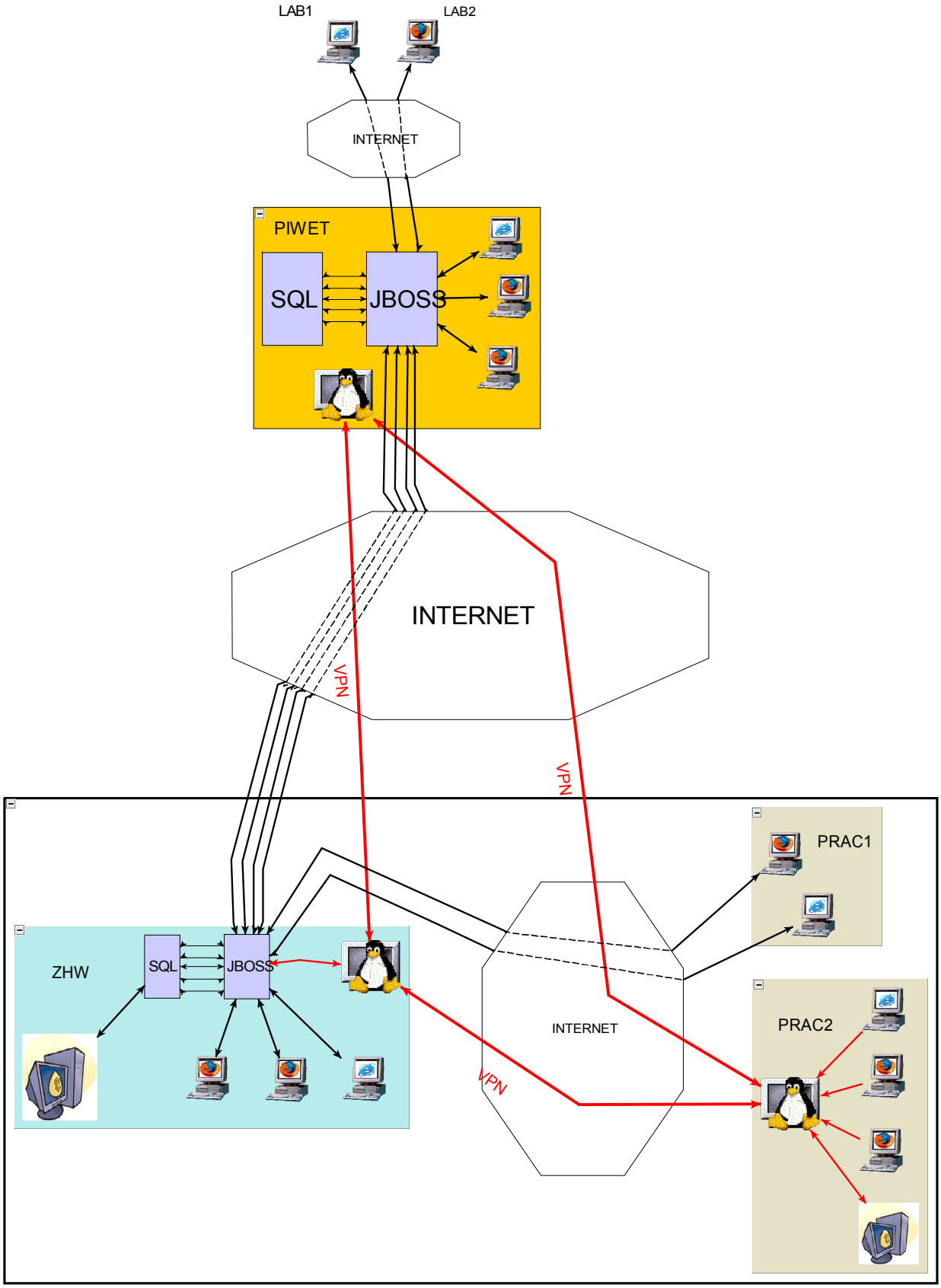
Osobną, nieujętą w tabeli funkcją, jest rejestracja próbek w terenie, która ze względu na swoją specyfikę została potraktowana jako niezależny moduł.

Przyjęte zostały następujące założenia dotyczące architektury systemu CELAB LIMS:

- System został opracowany w architekturze mieszanej (klient-serwer oraz cienkiego klienta).
- W szesnastu lokalizacjach w kraju (po jednej na każdy wojewódzki ZHW) zostały posadowione serwery z oprogramowaniem CELAB LIMS. Na każdym serwerze została uruchomiona samodzielna baza danych PostgreSQL oraz samodzielny serwer aplikacji JBoss. Na serwerze został zainstalowany system PLD Linux.
- W zależności od potrzeb zostały wdrożone cztery możliwe koncepcje dostępu do oprogramowania CELAB:
    - Uruchomienie samodzielnej aplikacji na komputerze z systemem Windows zlokalizowanym bezpośrednio w ZHW i bezpośrednie połączenie z bazą danych działającą w sieci LAN (technologia klient-serwer).
    - Uruchomienie w przeglądarce internetowej aplikacji intranetowej uruchomionej na serwerze w sieci LAN (technologia przeglądarkowa).
    - Uruchomienie na komputerze w laboratorium lub pracowni zewnętrznej aplikacji w przeglądarce internetowej (bezpośrednio przez Internet po bezpiecznym połączeniu SSL - technologia przeglądarkowa).
    - Zestawienie szyfrowanego tunelu z lokalizacji zewnętrznej do ZHW, a tym samym skonfigurowanie wirtualnej sieci prywatnej VPN (przy użyciu technologii IPSec lub OpenVPN). W przypadku zestawienia VPN dostęp do aplikacji CELAB jest możliwy na każdy z trzech wyżej wymienionych sposobów.
- Według przyjętego powyżej podziału zadań realizowanych przez moduł CELAB LIMS przyjęta została koncepcja implementacji odpowiedniej funkcjonalności w technologii klient-serwer oraz przeglądarkowej. W ogólnym zarysie funkcje związane z rejestracją badań laboratoryjnych i obsługą laboratorium zostały zaimplementowane w technologii przeglądarkowej. Natomiast funkcje związane z rozrachunkami, rozliczeniami, kasą i bankiem zostały zaimplementowane w technologii klient-serwer. Za takim podziałem implementacji przemawiają cechy takie jak łatwość i skalowalność realizacji technologii przeglądarkowej, mobilność tej technologii oraz łatwość wprowadzania zmian w rozwijającym się systemie, ale także różnica w szybkości wprowadzania danych na korzyść technologii klient-serwer, zaawansowane możliwości raportowania tej technologii oraz uniwersalność funkcji bibliotecznych.
  Zakres funkcjonalności obsługiwanej przez moduły CELAB LIMS zrealizowane w obu technologiach nie jest całkowicie rozłączny. Część funkcji działa w sposób równoważny w obu wersjach. Zaznaczyć też należy, że obie wersje wykorzystują ten sam mechanizm bazy danych i korzystają z dokładnie tych samych informacji systemowych.
- Wymiana danych między systemami CELAB LIMS w ZHW a systemem CELAB CBD w Puławach jest realizowana na zasadzie automatycznych transmisji danych w formacie XML. Większość transmisji jest inicjowana automatycznie przez system. Zminimalizowanie niezbędnych interwencji ze strony użytkowników pozwala na utrzymanie optymalnej aktualności i spójności informacji. Rolę człowieka w tak skomplikowanym, dwukierunkowym procesie replikacyjnym ograniczono do kontroli i weryfikacji prawidłowości przebiegu zadań automatycznych. Uprawnieni użytkownicy mają możliwość ręcznego inicjowania transmisji.

3.3. Szczegółowy schemat architektury systemu

Koncepcję architektury całego systemu przedstawia poniższy schemat:



Na rysunku przedstawiono podstawowe koncepcje:

- Zrealizowane przy użyciu routerów linuxowych połączenie VPN między różnymi lokalizacjami, zapewniające możliwość bezpiecznej pracy w jednej wirutalnej sieci prywatnej

(na schemacie kolor czerwony łączący PIWET, ZHW i PRAC2),

- Możliwość zdalnej pracy przez Internet w aplikacji CELAB CBD przez zewnętrzne, samodzielne laboratoria (na schemacie LAB1 i LAB2),
- Możliwość zdalnej pracy przez Internet w aplikacji CELAB LIMS przez zewnętrzne pracownie ZHW (na schemacie PRAC1 i PRAC2),
- Zaznaczamy, że połączenie VPN pomiędzy samodzielnymi pracowniami (PRAC2) a PIWET nie służy normalnemu trybowi pracy, gdyż odbywa się ono za pośrednictwem lokalnego serwera w ZHW.

3.4. Moduł statystyczny

Do realizacji modułu statystycznego wykorzystano następujące technologie:

- Projekt R - środowisko oraz język do obliczeń statystycznych. Jest to otwarte (dostępne na licencji Open Source), kompletne środowisko obliczeniowe przeznaczone do realizacji rozmaitych zadań analizy statystycznej. Środowisko języka R można rozszerzać o własne funkcje, algorytmy i biblioteki, a ogólnodostępna biblioteka CRAN zapewnia bardzo szeroki zakres gotowych rozwiązań wielu zadań współczesnej statystyki.
- PL/R - implementacja języka R dla bazy danych PostgreSQL.

Powyższe rozwiązanie umożliwia wykorzystanie złożonych funkcji statystycznych w standardowych zapytaniach języka SQL bazy PostgreSQL. Zapewnia możliwość korzystania zarówno z funkcji wbudowanych i bibliotecznych, jak i możliwość zaprogramowania własnych rozwiązań obliczeniowych. Otwartość rozwiązania gwarantuje praktycznie nieograniczone możliwości rozbudowy modułu i dostosowania do indywidualnych potrzeb. Integracja z bazą danych zapewnia natomiast optymalną wydajność przetwarzania danych.

Przygotowanie analiz statystycznych już na poziomie bazy danych umożliwia łatwą integrację modułu statystycznego z systemem raportów i wydruków aplikacji CELAB. Pozwola na łatwe generowanie raportów tabelarycznych i graficznych w różnych formatach. Umożliwia też między innymi przygotowanie gotowych raportów statystycznych w trybie wsadowym (automatycznie i okresowo wg. zdanych parametrów)

Oparcie bazy centralnej i baz lokalnych (wojewódzkich) o bliźniaczą strukturę danych umożliwia zastosowanie tych samych narzędzi do generowania raportów i analiz statystycznych zarówno dla aplikacji centralnej (CBD) i lokalnej (LIMS). Do zastosowań wojewódzkich wystarczają gotowe szablony raportów i nie potrzebne jest wykorzystywane wszystkie możliwości środowiska Projektu R. Zaawansowani użytkownicy dobrze znający temat obliczeń statystycznych mogą wykorzystywać w pełni możliwości jakie daje otwarte rozwiązanie.

W przypadku aplikacji CELAB LIMS, standardowe analizy związane z kontrolą jakości (m.in. karty kontrolne Shewharta) są łatwo dostępne jako gotowe do wykorzystania raporty. Wszystkie obliczenia statystyczne (wartość średnia, odchylenie standardowe, skośność, kurtoza, przedział ufności i inne) wykonane są automatycznie.

4. Platforma programowo-sprzętowa

Na wszystkich serwerach systemem operacyjnym jest Linux. Linux jest jednym z najlepszych systemów operacyjnych. Według opinii powszechnie przyjętej w świecie profesjonalnych zastosowań technologii informatycznych, Linux zapewnia stabilność i bezpieczeństwo. Są to główne kierunki działań programistów Linuxa, rozwijających jądro systemu (kernel) i aplikacje.

Kod Linuxa i programów, oparty o licencję GNU/GPL jest otwarty. Dzięki temu w pracę nad Linuxem i aplikacjami dla systemu Linux mogło zaangażować się wiele setek tysięcy programistów.

Ma to też tę konsekwencję, że w przypadku odkrycia luki w systemie, czas jej usunięcia (stworzenia tzw. "łatki") jest krótszy, niż w przypadku oprogramowania komercyjnego.

5. Bezpieczeństwo

5.1. IPSec

W projekcie zostało zastosowane tunelowanie połączeń sieciowych oparte na protokole IPSec. Dwoma podstawowymi zadaniami IPSec jest zapewnienie integralności oraz poufności danych przesyłanych przy pomocy internetowego protokołu IP. Poufność, czyli brak możliwości odczytania przechwyconych przez napastnika danych bez znajomości odpowiedniego klucza, jest zapewniana przez algorytmy kryptograficzne w postaci szyfrów blokowych takich jak DES.

Rozszyfrowaniem i weryfikacją integralności otrzymanych z sieci danych zajmuje się system operacyjny, a dane trafiają do aplikacji, która nie musi nic wiedzieć o protokole IPSec.

Tzw ,,bezpieczny tunel" (SA) , jest jednym z podstawowych pojęć leżących u podstaw architektury IPSec. Jest to jednokierunkowy kanał, którego końcami są dwa hosty, identyfikowany przez unikalny numer SPI (Security Parameters Index). Na numer SPI składa się cały zestaw parametrów, charakteryzujących dany kanał (algorytm szyfrujący, algorytm uwierzytelnienia, ,,okno" chroniące przed powtarzaniem pakietów, okres ważności i in.) znanych wyłącznie hostom będącym końcami tunelu. SPI jest dowolną, 32-bitową liczbą, ustalaną przez administratora podczas ręcznej konfiguracji tunelu, lub wybieraną losowo w razie konfiguracji automatycznej. Identyfikator ten jest jedynym charakterystycznym parametrem tunelu, który jest widziany przez osobę potencjalnie podsłuchującą łącza. Informacja ta ma znaczenie (algorytm szyfrujący itp.) wyłącznie dla routerów, stanowiących końce tunelu. W projekcie został zastosowany mechanizm automatycznej konfiguracji bezpiecznych tuneli IPSec.

Protokół IPSec stanowi integralną część jądra systemu Linux. W ramach projektu CELAB została wykorzystana otwarta implementacja OpenSWAN i standardowe mechanizmy jądra Linuxa w wersji 2.6.

5.2. Open VPN

VPN czyli wirtualna sieć prywatna (Virtual Private Network) zapewnia bezpieczną transmisję danych pomiędzy niezależnymi sieciami lokalnymi LAN. Transmisja przebiega poprzez szyfrowany tunel w sieci Internet. Podstawową realizacją VPN jest tunelowanie IPSec (patrz rozdzaił: 5.1. IPSec). W szczególnych przypadkach, gdy utworzenie stałych tuneli IPSec nie było możliwe (brak stałego adresu IP, brak możliwości skonfigurowania routera linuxowego) wykorzystano oprogramowanie OpenVPN, które realizuje bezpieczne tunelowanie połączeń dla samodzielnych stacji roboczych z systemem operacyjnym Windows 2000/XP.

Konfiguracja VPN pozwala na udostępnienie określonym grupom informacji z baz danych systemu CELAB. Zapewnia również bezpośredni, zdalny dostęp do stacji roboczych, ułatwiający administrację i uaktualnianie oprogramowania przez zewnętrznych administratorów sieci.

5.3. SSL

Wszystkie usługi oparte o technologię webową zostały zabezpieczone przez protokół SSL (ang. Secure Sockets Layer), zapewniający poufność i integralność transmisji danych oraz bezpieczeństwo uwierzytelnienia. SSL oparty jest na szyfrach asymetrycznych oraz tzw. certyfikatach standardu X.509. Protokół ten jest obsługiwany przez wszystkie wykorzystywane przeglądarki internetowe.

5.4. Hasła

System CELAB wymaga od użytkowników korzystania z bezpiecznych haseł. Bezpieczne hasło to takie, które składa się z co najmniej ośmiu znaków, zawiera kombinację wielkich i małych liter, cyfr oraz symboli specjalnych a także jest łatwe do zapamiętania, lecz trudne do odgadnięcia przez innych. System wymusza wprowadzanie haseł o odpowiednim poziomie bezpieczeństwa zgodnie z powyższymi zaleceniami. Nie pozwola na wpisanie hasła zbyt krótkiego lub zbyt prostego.

5.5. Uprawnienia, kontrola dostępu

Każdy użytkownik w systemie posiada własne hasło i przydzielone uprawnienia. Uprawnienia te

przydziela administrator systemu i tylko on może je modyfikować. Umożliwia to kontrolę dostępu użytkowników do określonych modułów i zasobów.

Kolejnym elementem polityki bezpieczeństwa są karty zbliżeniowe oraz odpowiednie czytniki. W ten sposób jest kontrolowany dostęp pracowników do budynków, pomieszczeń itp.. Rozwiązanie takie zabezpiecza przed nieautoryzowanym dostępem do informacji przez osoby obce.

5.6. Zabezpieczenie sieci wewnętrznej (tzw. firewall)

Konfiguracja "ściany ogniowej" została wykonana w oparciu o standardowe mechanizmy zawarte w jądrze systemu Linux – iptables.

Konfiguracja serwerów udostępnia na zewnątrz jedynie niezbędne i wykorzystywane usługi, przy jednoczesnym blokowaniu wszystkich innych usług wewnętrznych. Konfiguracja taka zapewnia izolację sieci wewnętrznych oraz zabezpieczenie serwerów przed niepowołanym dostępem. Jednocześnie firewall jest podstawą działania przezroczystego serwera proxy (transparent proxy), wirtualnych sieci prywatnych (VPN) oraz udostępniania Internetu dla komputerów wewnątrz sieci LAN. Zastosowany firewall umożliwia stworzenie tzw. maskarady (posługującej się niepublicznymi adresami IP), która dodatkowo izoluje od sieci Internet.

5.7. Bezpieczny i szybki dostęp do stron WWW

Dostęp do internetowych stron WWW dla użytkowników z sieci wewnętrznej został zrealizowany przez tzw. serwer pośredniczący Proxy. W tym celu wykorzystano popularny programu Squid, ze wzgledu na fakt, iż daje on duże możliwości konfiguracji i znacząco zmniejsza obciążenie łącza. Sprzyja to szybszemu dostępowi do Internetu. Serwer pośredniczący działa na zasadzie przezroczystego proxy (transparent proxy), nie wymaga więc żadnej konfiguracji na stacjach roboczych użytkowników. Serwer pośredniczący Squid pozwala na ustawienie szeregu opcji dostępu do różnego rodzaju zasobów (głównie stron WWW z różnych domen internetowych) oraz na regulowanie dostępu do tych zasobów na poziomie pojedynczych komputerów w sieci wewnętrznej. Pozwala to wprowadzić ściśle określoną politykę udostępniania zasobów dla poszczególnych użytkowników oraz grup użytkowników.

6. Technologie programistyczne

6.1. Biblioteki FINN

Aplikacja została oparta o sprawdzone i przetestowane biblioteki narzędziowe Framework FINN firmy FINN Sp. z o.o. Wybrane rozwiązanie zapewnia obsługę szkieletowych funkcji programu oraz wszystkich podstawowych poleceń systemowych, w tym:

- autentykacji i autoryzacji,
- użytkowników i grup,
- uprawnień,
- archiwizacji,
- generatora wydruków,
- replikacji i integracji,
- podstawowych elementów interfejsu graficznego.

6.2. J2EE

Wersja przeglądarkowa programu CELAB została oparta o technologię J2EE firmy Sun. Java 2 Enterprise Edition (J2EE) definiuje standard tworzenia aplikacji w architekturze wielowarstwowej. J2EE wykorzystuje język Java jako podstawę programowania logiki aplikacji oraz definiuje środowisko wykonania i model aplikacji. Wykorzystywaną technologią komponentową jest EJB (Enterprise Java Beans). Architektura Enterprise Java Beans jest architekturą przeznaczoną do tworzenia aplikacji bazujących na rozproszonych komponentach, wspierających transakcje. Jest to specyfikacja, która określa strukturę usług działających po stronie serwera i jest ona przeznaczona dla

producentów, którzy implementują w swoich serwerach środowisko EJB.

6.3. JSP

Java Server Pages (JSP) to technologia bazująca na języku Java umożliwiająca szybkie i łatwe tworzenie dynamicznych stron internetowych. Pliki JSP są plikami HTML wraz z kodem źródłowym Javy zawartym w specjalnych znacznikach. Dość istotnym jest fakt, iż kod plików JSP nie jest czytany linia po linii (jak ma to miejsce na przykład w przypadku popularnej technologii PHP) lecz najpierw konwertowany do postaci tzw. servletu (postać binarna), a następnie uruchamiany przez tzw. silnik servletów (servlet container, np. JBoss).

6.4. PowerBuilder

PowerBuilder to prosty w użyciu obiektowy język programowania czwartej generacji. Umożliwia dostęp do setek wbudowanych funkcji. Służy do budowy aplikacji klient/serwer, wielowarstwowych, rozproszonych i internetowych. Wyposażony został w dedykowane sterowniki do baz danych oraz zawiera moduł CASE do fizycznego modelowania danych.

PowerBuilder umożliwia pisanie własnych funkcji lub korzystanie z istniejących napisanych w C++ lub innym języku, udostępnianych w plikach DLL. Za pomocą PowerBuilder Native Interface można łączyć aplikacje napisane w PowerBuilderze z aplikacjami napisanymi w innych językach (C, Java). PowerBuilder posiada standardowe cechy narzędzia obiektowego: wielopoziomowe dziedziczenie, hermetyzacja danych i funkcji oraz polimorfizm.

Debuger z intuicyjnym, graficznym interfejsem użytkownika podnosi komfort i efektywność pracy programistów. Interfejs użytkownika składa się z wielu dostosowywalnych paneli umożliwiających m.in. przeglądanie kodu aplikacji, punktów przerwań i podgląd zmiennych. W oparciu o dane wprowadzone przez użytkownika, kreatory PowerBuildera automatycznie tworzą funkcjonalny szkielet komponentu, projekt aplikacji oraz dostosowywalną listę czynności „do zrobienia”.
Narzędzia do monitorowania obciążenia poszczególnych części aplikacji umożliwiają identyfikację „wąskiego gardła” programów i optymalizację wydajności. Dołączone biblioteki klas, PowerBuilder Foundation Class, oraz przykładowe aplikacje pomagają w szybkim prototypowaniu i konstrukcji oprogramowania. Obsługa zestawu znaków Unicode umożliwia tworzenie aplikacji wielojęzycznych.
PowerBuilder zawiera dedykowane sterowniki pozwalające na bezpośredni dostęp do najbardziej rozpowszechnionych systemów relacyjnych baz danych.

Opatentowana technologia DataWindow umożliwia manipulację danymi i prezentację informacji z baz danych. Wbudowany serwer bazy danych Sybase Adaptive Server Anywhere umożliwia natychmiastowe rozpoczęcie prac nad rozwojem aplikacji. Technologia Data Pipeline pozwala na migrację danych poprzez kopiowanie definicji tablic i danych z jednej bazy do drugiej, nawet jeśli dane te znajdują się w różnych systemach bazodanowych.

7. Wymiana danych

7.1. Współpraca z innymi systemami

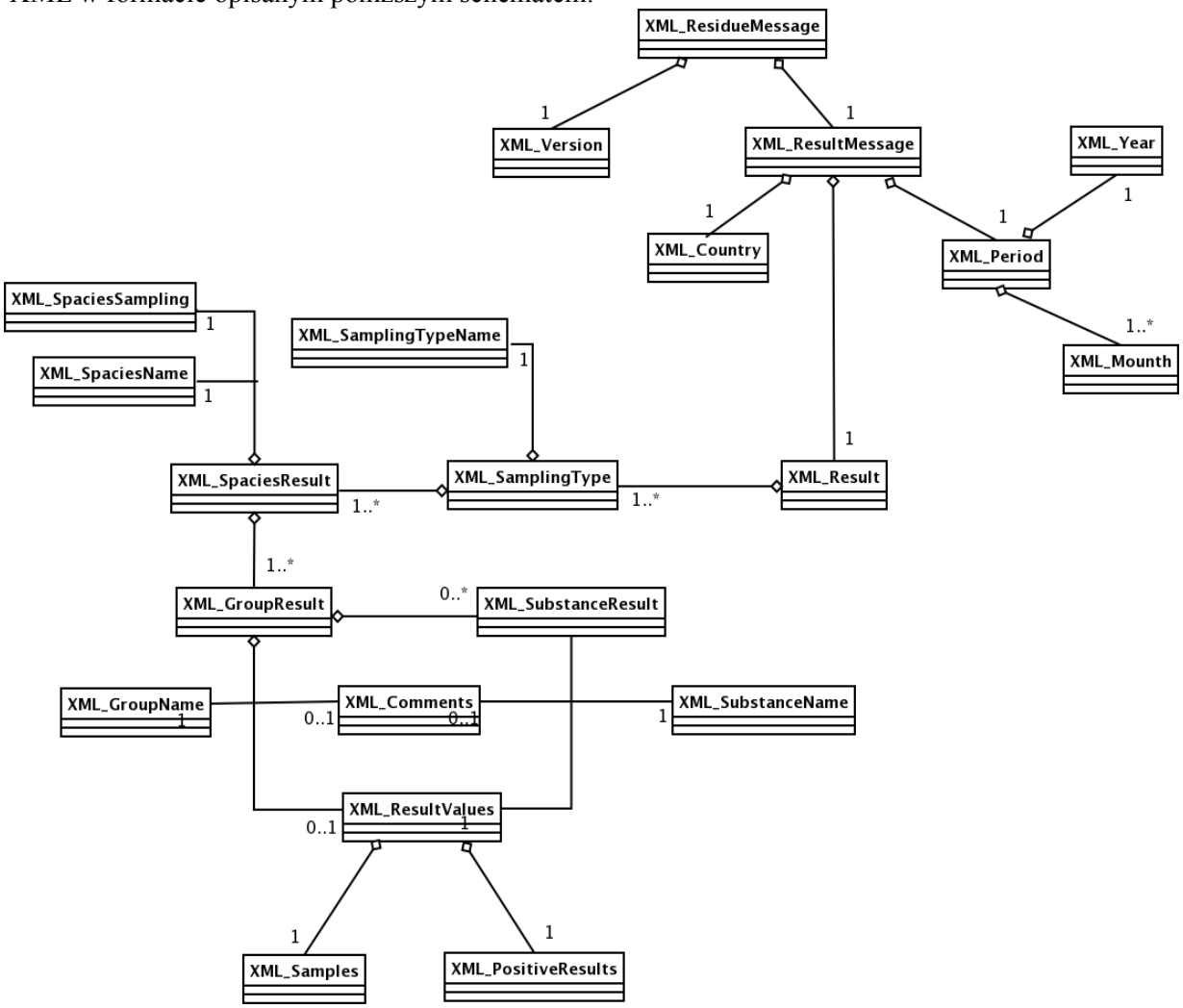
System CELAB współpracuje z innymi systemami informatycznymi już wdrożonymi bądź takimi, które dopiero będą wdrażane w jednostkach uczestniczących w projekcie. Integracja jest jednym z podstawowych czynników zapewniających spójność informacji, jest więc niewątpliwie czynnikiem niezwykle istotnym dla głównych celów niniejszego systemu. Współpraca jest realizowana na wielu poziomach i dotyczy wielu modułów oprogramowania CELAB. Systen CELAB wykorzystuje formatu XML, który jest formatem nowoczesnym i zapewniającym największą elastyczność. Wykorzystanie XML do importów i eksportów danych zapewnia:

- uniezależnienie się od konkretnych implementacji programowych,
- możliwość pełnej kontroli wysyłanych informacji,
- bezproblemową obsługę polskich znaków diaktrycznych w jednolitym kodowaniu (np. UTF),
- współpracę z wieloma programami wykorzystującymi format XML,

- możliwość łatwej modyfikacji i adaptacji formatu przesyłania danych przy wykorzystaniu transformacji XSLT,
- możliwość kontroli podstawowej spójności informacji już na etapie pliku transmisyjnego (DTD, XML Schema).

7.2. Współpraca na poziomie aplikacji CBD

System centralnej bazy danych oprócz swojej głównej funkcji jaką jest pobieranie danych z aplikacji laboratoryjnej współpracuje również z innymi systemami informatycznymi wykorzystywanymi głównie przez inspekcję weterynaryjną w tym z europejskim systemem NRCP do kontroli badań pozostałości, który już w chwili obecnej obsługuje przyjmowanie danych w formacie XML w formacie opisanym poniższym schematem:



Istotnym elementem jest import danych z programów rejestracji badań wykorzystywanych przez samodzielne laboratoria. Ważnymi cechami transmisji danych są:

- wykorzystanie plików XML w formacie ustalonym przez schemat XSD,
- wykorzystanie plików XML kodowanych w UTF-8,
- transmisja szyfrowana przez SSL,
- elastyczna specyfikacja pól bazy danych - możliwość adaptacji algorytmu obsługującego odbieranie informacji w zależności od faktycznie przekazywanych danych. Umożliwia to bezproblemowe przyjmowanie danych w miarę uzupełniania systemu centralnego o nową funkcjonalność.

- alternatywne wprowadzanie danych ręcznie przez formularz na stronie internetowej.

7.3. Współpraca na poziomie aplikacji LIMS

W przypadku aplikacji do obsługi laboratorium CELAB LIMS zakres współpracy z innym oprogramowaniem jest potencjalnie bardzo szeroki. Podstawowymi aspektami takiej współpracy są:

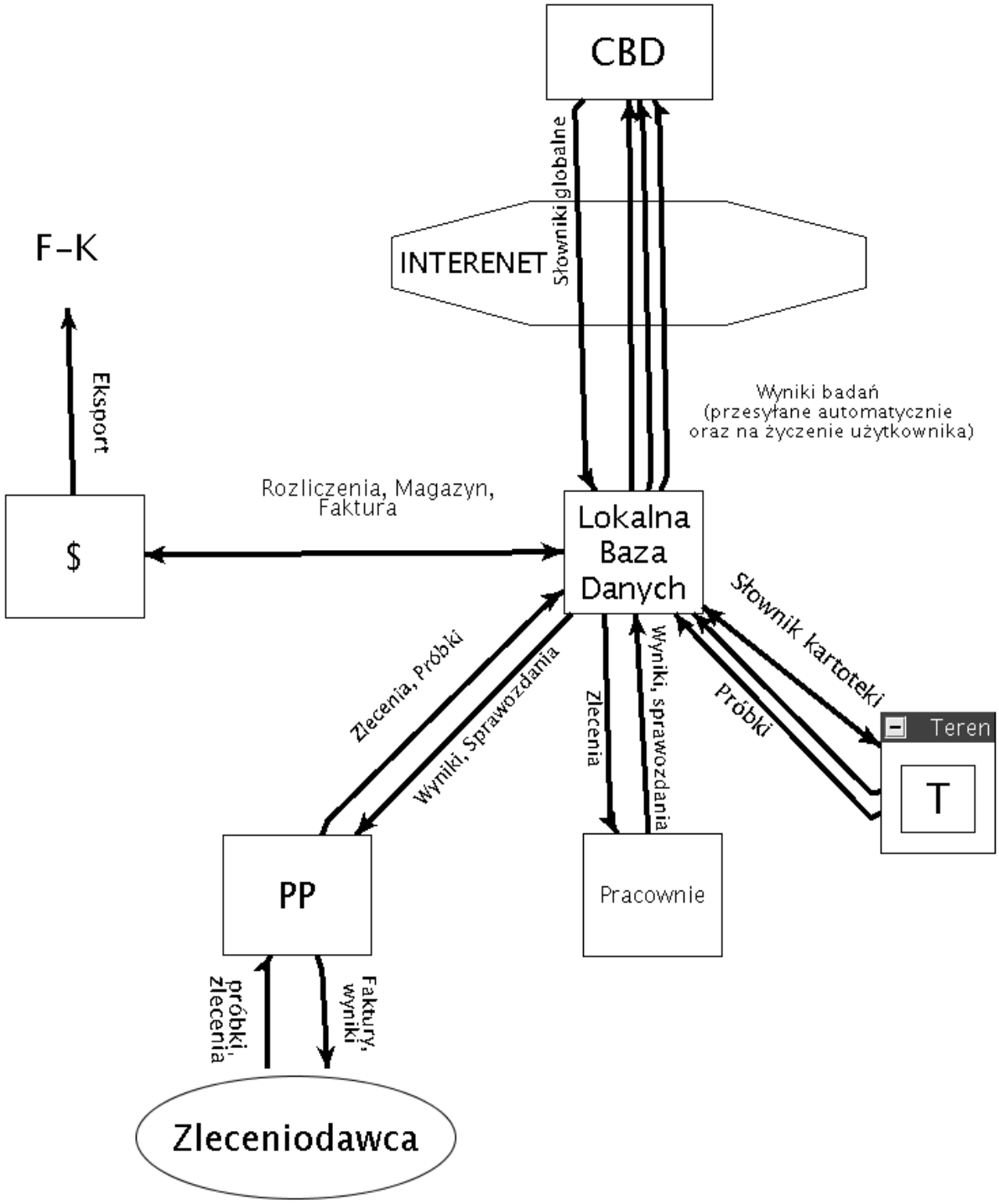
- wykorzystanie plików XML w formacie ustalonym przez schemat XSD wszędzie tam, gdzie jest to możliwe i zasadne,
- wykorzystanie plików XML kodowanych w UTF-8 wszędzie tam, gdzie jest to możliwe i zasadne,
- obsługa innych formatów danych tylko w przypadkach braku możliwości wykorzystania XML,
- przeniesienie danych z aktualnie wykorzystywanych programów rejestracji badań i wyników oraz obsługi laboratorium wykorzystywanych w ZHW będzie operacją jednorazową, dedykowaną pod konkretne rozwiązanie dostosowane do ilości przenoszonych danych,
- wysyłanie wszelkich powiadomień (w tym powiadomień o wynikach dodatnich) w formacie poczty elektronicznej,
- obsługa sprzętu laboratoryjnego w zakresie automatycznego pobierania danych o wykonanych badaniach,
- eksport danych z systemu obsługi sprzedaży i fakturowania do zewnętrznych systemów finansowo-księgowych (ulokowanych najczęściej poza ZHW).

7.4. Wymiana danych między modułami systemu CELAB

Przy projektowaniu współpracy poszczególnych modułów systemu CELAB wzięto pod uwagę te same czynniki, które stanowią o zaletach formatu XML przy transmisji danych. W związku z powyższym praktycznie wszystkie rodzaje wewnętrznej transmisji danych między modułami oprogramowania zostały oparte o XML. Wymienić można kilka podstawowych rodzajów transmisji danych w ramach systemu CELAB:

- przesyłanie danych o wynikach badań z aplikacji LIMS do aplikacji CBD,
- przesyłanie słowników globalnych z aplikacji CBD do aplikacji LIMS,
- przesyłanie informacji o zebranych próbkach z systemu terenowej rejestracji próbek do modułem LIMS,
- wymiana (synchronizacja) lokalnych słowników i kartotek między aplikacją LIMS a systemem do rejestracji próbek w terenie.

Ogólny schemat koncepcji przesyłania informacji między różnymi modułami przedstawia poniższy schemat:



Objaśnienia:

- PP - punkt przyjęć przyjmujący od Zleceniodawcy próbki i wydający mu wyniki badań oraz wystawiający faktury, oraz wprowadzający do lokalnej bazy danych zlecenia,
- Pracownie - pracownie laboratoryjne ZHW w których na podstawie wprowadzonych zleceń przeprowadza się badania i ich wyniki wprowadza do bazy danych,
- Teren - moduł rejestracji badań w terenie wprowadzający próbki do lokalnej bazy danych,
- $ - moduł zarządzania laboratorium prowadzący rozliczenia i magazyny oraz tworzący raporty i zestawienia dla systemu finansowo-księgowego (FK),

Z Centralnej Bazy Danych do baz lokalnych przesyłane są aktualizacje słowników globalnych,

Z baz lokalnych do CBD przesyłane są wyniki badań.

Należy zwrócić szczególną uwagę na możliwość dostosowania wszelkich mechanizmów eksportów do zmieniających się potrzeb. W szczególności ważnym elementem systemu jest możliwość definiowania i uzupełniania przez uprawnionych i przeszkolonych użytkowników zakresów eksportowanych danych.

7.5. Wydruki i raporty

Jednym z istotnych elementów systemu jest mechanizm wydruków i raportowania. Wydruki i raporty generowane są w postaci plików Adobe PDF w oparciu o szablony opisane w języku XML. Takie podejście ma następujące zalety:

- wszystkie wydruki mają profesjonalny, elegancki wygląd,
- oprócz natychmiastowego wydruku na drukarce, raporty w postaci plików PDF można zapisać na dysku do późniejszego wydruku lub przesłać je drogą elektroniczną do innych osób,
- pliki PDF można odczytać praktycznie na każdym komputerze z każdym systemem operacyjnym,
- pliki PDF mogą być automatycznie podpisane przez systemu przy użyciu kryptograficznego certyfikatu, gwarantującego autentyczność dokumentu,
- wydruki w postaci plików PDF są niezależne od zainstalowanej w systemie drukarki,
- wydruki i raporty mogą zawierać elementy graficzne (ikony, symbole, wykresy itp.),
- XML'owe szablony wydruków można modyfikować przy użyciu prostego w obsłudze i darmowego oprogramowania.

Określone raporty i wydruki można generować w innych formatach. Mogą to być pliki XML zawierające dane, które nadają się do automatycznego przetwarzania przez inne systemy informatyczne. Mogą to być również pliki RTF, które mogą być użyte w dokumentach tworzonych w typowym oprogramowaniu biurowym (Microsoft Office, Open Office).

Osobnym tematem jest generowanie wydruków przedstawiających elementy w zależności od lokalizacji geograficznej (na mapach konturowych). W tym przypadku wykorzystany został nowoczesny i otwarty format grafiki wektorowej SVG.

Bardzo skomplikowane raporty (w szczególności centralne raporty statystyczne) są generowane dwuetapowo. W pierwszym etapie, wykonywanym automatycznie okresowo lub na żądanie, informacje są grupowane w metadane. W drugim etapie na podstawie metadanych są generowane właściwe raporty. Takie rozwiązanie pozwola skrócić czas oczekiwania zaawansowanych użytkowników na wyniki złożonych obliczeniowo operacji.

8. Struktura bazy danych

Struktura bazy danych **CELAB** została zamieszczona w pliku ***Struktura bazy danych.html***. Jest przechowywana i aktualizowana na płycie CD.

Projekt struktury bazy danych o badaniach laboratoryjnych opiera się na założeniu, że fizyczna struktura bazy centralnej ma być taka sama jak fizyczna struktura bazy lokalnej. Przyjęto rozwiązanie gwarantujące maksymalną elastyczność przy definiowaniu zakresu gromadzonych danych zarówno w bazie lokalnej jak i bazie centralnej. Wynika to z następujących rozwiązań:

- Wszystkie dane o zleceniach, próbkach, badaniach i ich wynikach są gromadzone w odpowiednich tabelach, które mają zdefiniowane fizycznie pola odpowiadające najważniejszym parametrom tych danych (pola główne),
- W zależności od rodzaju zlecenia, rodzaju próbki, rodzaju badania i rodzaju wyniku (metody badawczej) możliwe jest włączanie i wyłączanie widoczności pól głównych oraz ustalanie ich wartości domyślnych, minimalnych i maksymalnych na etapie konfiguracji systemu,
- W zależności od rodzaju zlecenia, rodzaju próbki, rodzaju badania i rodzaju wyniku (metody badawczej) możliwe jest definiowanie nowych pól (typu tekstowego, numerycznego, daty lub

słownikowego) oraz ich wartości domyślnych, minimalnych i maksymalnych na etapie konfiguracji systemu,

- W przypadku pól definiowanych można określić długość pola tekstowego oraz liczbę miejsc po przecinku i formułę przeliczenia wyniku w przypadku pola numerycznego.
- W przypadku pól numerycznych przewidziana została możliwość wprowadzania specjalnych wartości w przypadku gdy danej nie da się jednoznacznie zapisać za pomocą liczby (np. gdy wynik nie mieści się w zakresie oznaczalności, gdy przekracza normy itp).

Dzięki takiemu podejściu możliwe jest wygodne rozwijanie programu według zmieniających się wymagań oraz łatwe dostosowanie do dedykowanych potrzeb poszczególnych ZHW. Względnie proste struktury bazodanowe oparte o klucze obce pozwalają na wydajne pobieranie danych przez zapytania SQL.

Należy zaznaczyć, że wszystkie tabele przechowujące dane w systemie CELAB posiadają standardowo pola zawierające informacje o datach utworzenia i ostatniej edycji rekordów oraz o użytkownikach, którzy wykonali te operacje.

Ponadto:

- Wszystkie dane o osobach korzystających z systemu przechowywane są w kartotece (słowniku) personelu mprac1. W pozostałych tabelach umieszcza się klucze z tabeli personelu (nr PESEL lub unikalny systemowy kod).
- Wszystkie dane o klientach i kontrahentach przechowywane są w kartotece (słowniku) kontrahentów mknt1. W pozostałych tabelach umieszcza się klucze z tabeli kontrahentów (nr NIP lub unikalny systemowy kod). Istnieje możliwość wprowadzania danych kontrahenta tzw. "jednorazowego" (adresu i nazwy) bez rejestracji go w kartotece.
- Istnieje możliwość automatycznego importu bazy stad dla danego województwa z bazy ARiMR, w formacie prostego standardowego pliku tekstowego oddzielonego przecinkami (CSV). Plik w takim formacie można uzyskać przy wykorzystaniu standardowej funkcji eksportu z arkusza kalkulacyjnego MS Excel lub OpenOffice Calc.
- W systemie istnieje możliwość grupowania (klasyfikowania) personelu i kontrahentów w trzech różnych, niezależnych i hierarchicznych klasyfikacjach, które można dowolnie definiować i modyfikować.
- System oferuje wygodne elementy interfejsu graficznego do wprowadzania określonych typów danych (m. in. wybieranie daty z pomocą kalendarza, podpowiadanie nazw ulic, miejscowości, kodu TERYT po wprowadzeniu kodu pocztowego, formatowanie i automatyczna walidacja pól liczbowych, walidacja numerów PESEL, NIP, REGON, IBN, walidacja adresów e-mail i www).

W skład systemu wchodzą również gotowe moduły oprogramowania rodziny FINN 8 SQL w zakresie oprogramowania elektronicznego obiegu dokumentów, finansowo-księgowego, magazynowego, obsługi sprzedaży i zaopatrzenia.

9. Pozostałe rozwiązania informatyczne

9.1. Rejestracja czasu pracy

System CELAB zawiera moduł Ewidencji Czasu Pracy (ECP). Moduł ten współpracuje standardowo z czytnikami kart zbliżeniowych TANGO i umożliwia łatwą i wygodną rejestrację czasu pracy oraz ewidencję czasu pracy w warunkach szkodliwych. Oprócz tego moduł ten zawiera także rozwiązania związane z bezpieczeństwem - blokada logowania do systemu użytkowników nie zarejestrowanych przez odpowiednie urządzenie.

Warunkiem wdrożenia pełnej wersji tego modułu jest posiadanie odpowiedniej infrastruktury sprzętowej w laboratorium w ZHW.

Możliwa jest jednak również ręczna ewidencja czasu pracy personelu przez przeszkolonego pracownika z odpowiednimi uprawnieniami. Wykorzystanie tego modułu traktujemy jako opcjonalne w zależności od potrzeb i możliwości technicznych konkretnych ZHW.

9.2. Podpis cyfrowy

Wiele już przygotowanych mechanizmów systemowych aplikacji CELAB obsługuje podpisy elektroniczne (w tym certyfikaty kwalifikowane). Jednak ze względu na specyfikę rozwiązania przyjęto, że w miarę możliwości zostaną wykorzystane tanie (lub nawet darmowe) certyfikaty niekwalifikowane (na przykład wystawione przez ośrodek certyfikacji FINN). Ograniczenie wydatków na certyfikaty kwalifikowane jest w tym przypadku zasadne, ponieważ realizowane w systemie działania i ich efekty nie wymagają pełnych konsekwencji prawnych stosowania certyfikatów kwalifikowanych.

10. Słowniki

Spisy słowników znajdują się na płycie CD. Słowniki są „dynamicznym" elementem oprogramowania. Niektóre słowniki są możliwe do samodzielnej edycji przez użytkowników, część słowników jest zatwierdzana „odgórnie". Zatwierdzone do używania hasła słowników znajdują sie w oprogramowaniu.