Wykaz zbiorów danych tworzących księgi rachunkowe na komputerowych nośnikach danych programu LeftHand Pełna Księgowość produkcji firmy LeftHand Sp. z o.o.

Wykaz zbiorów danych

Głównymi zbiorami danych w programie LeftHand Pełna Księgowość są następujące pliki:

lh.gdb, stanowiący mechanizm linka symbolicznego; wskazuje na właściwe pliki z bazami gromadzonych danych

lh_ +symbol_firmy+ .gdb , plików tych jest tyle ile obs ugiwanych w programie firm. Stanowi on najważniejszy zbiór danych, ponieważ to w nim zapisywane są wszystkie informacje wprowadzane przez użytkowników. Plik jest binarną bazą danych standardu SQL obsługiwaną przez relacyjny (RDMS) system bazodanowy Firebird firmy Borland.

Powiązanie i funkcje zbiorów danych.

Po zainstalowaniu programu na dysku komputera tworzony jest automatycznie plik o nazwie lh.gdb , który stanowi bazę dzie zbiór wska ników na w a ciwe pliki z danymi firmy.

Dodając w programie LeftHand Pełna Księgowość nową firmę do obsługi tworzony jest właściwy plik bazodanowy o nazwie lh_ +symbol_firmy+ .gdb w lokalizacji ustawionej podczas instalacji programu. Ten plik jest właściwym magazynem danych, będącym relacyjną bazą SQL'ową. Takie rozwiązanie ma niewątpliwe wysoki współczynnik integralności i spójności danych.

Mechanizmy bezpieczeństwa danych

W programie LeftHand zastosowano wielostopniowy różnorodny system zabezpieczania danych gromadzonych w bazie danych firmy. Wyróżnić możemy następujące mechanizmy bezpieczeństwa:

1. **Dostęp osób upoważnionych do danych księgowych i handlowych**
   Podczas uruchomienia programu konieczne jest podanie właściwego loginu i hasła dostępowego do wybranych modułów i funkcjonalności programu. Login i hasło mogą mieć na tyle długie wartości aby można było zdefiniować je w sposób uniemożliwiający dostęp do programu za pomoc a tzw. metod brut force . Has em zabezpieczony jest również panel administracyjny służący do konfiguracji technicznej parametrów baz danych.
2. **Restrykcyjny system uprawnień**
   Administrator systemu po konsultacji z kierownikiem jednostki, bazując na kompetencjach konkretnych pracowników, może przygotować dla konkretnego pracownika opisanego w programie loginem i hasłem tzw. rolę , b d ca zbiorem uprawnie do wybranych modu ów

i ich funkcjonalności

3. **Zabezpieczenie dostępu do bazy danych SQL**
   Użytkownik ma możliwość zmiany domyślnego hasła fizycznego dostępu do bazy danych SQL, w której przechowywane są wszystkie wprowadzane dane, tak aby zabezpieczyć się przed ewentualną próbą pozyskania danych przez osoby trzecie
4. **Zabezpieczenia strukturalne**
   Oprócz zabezpieczeń zewnętrznych dane są zabezpieczane wewnątrz bazy danych poprzez zestaw funkcji nazywanych triggerami, które mają na celu kontrolowanie spójności i poprawności gromadzonych danych. Dodatkowo każdy z modułów posiada indywidualne mechanizmy kontroli spójności w zakresie modyfikacji, usuwania i powiązań pomiędzy zbiorami danych