Lekcja: Zabezpieczenia dostępu do danych (zarządzenie bezpieczeństwem).

1. Polityka bezpieczeństwa w SZBD sprowadza się do właściwego określania dostępności, spójności oraz poufności. Dostępność określa jak najlepszy dostęp do danych, dla których użytkownik ma przyznane uprawnienia. Spójność określa ograniczenia, które posiadają użytkownicy, mówi o tym jakie operacje może wykonywać, a jakie są zabronione (*np. nie może zmieniać hasła*). Poufność natomiast wskazuje na dostęp użytkowników tylko do tych danych, z których mogą oni korzystać, oraz blokuje dostęp do danych dla nich nieprzeznaczonych.
2. W systemach bazodanowych uprawnienia może nadawać administrator korzystając z klauzuli SQL „GRANT". Poza tym użytkownik o większych uprawnieniach może odbierać lub nadawać uprawnienia użytkownikom o mniejszych prawach klauzulą „REVOKE"(*np. na forach internetowych, ja jestem administratorem witryny, a na niej logują się administratorzy danych tematów, poza tym są jeszcze moderatorzy*). System ten nosi nazwę uznaniowego. W wielu systemach bazodanowych definiuje się także role, które określają zestaw uprawnień i ograniczeń dla wyznaczonej grupy użytkowników. Role definiuje się za pomocą klauzuli „SQL SET ROLE".
3. W bazach danych można stosować kategorie bezpieczeństwa oparte na modelu Bell-LaPadula:

Kategorie dostępu do informacji	Angielskie	Oznaczenie umowne
Ściśle tajne	Top secret	A
Tajne	Secret	B
Pufne	Confidential	C
Do użytku wewnętrznego	Restricted	D
Jawne	Unclassified	E

   W modelu tym kategorie bezpieczeństwa są uporządkowane liniowo. Każdy pomiot ma określony poziom uprawnień. Prawo odczytu informacji jest możliwe (dziedziczone) w dół, nigdy w górę. Możliwy jest przepływ informacji w górę (*tzn. podmiot może pisać do obiektu nad nim*). Podmiot z przypisanym poziomem uprawnień nie może komunikować się z podmiotem, który nie ma przypisanego poziomu uprawnień.

   Model ten zapewnia spójność danych (*kto ma dostęp i do czego*). Nie określa natomiast kontroli dostępu, nie określa mechanizmów zmian praw dostępu, nie rozwiązuje problemu plików współdzielonych.
4. W celu uzyskanie dostępu do bazy danych użytkownik musi się zalogować. SZBD za pomocą klauzul SQL „grant" i „revoke" przyznaje dostęp do danych. Serwer MySQL przechowuje informacje o uprawnieniach w swojej wewnętrznej bazie „mysql". Uprawnienia te mają postać kolumn o typie „enum" i wartościach „N" lub „Y", wskazujących na brak uprawnień lub ich przyznanie. Tabela w bazie „mysql" o nazwie „user" przechowuje informacje o hasłach użytkowników w kolumnie

password, które są szyfrowane algorytmem MD5. Same pliki to „user.MYI”, „user.frm” oraz user.MYD” – ten przechowuje hasła.