# Temat projektu: **wypożyczalnia samochodowa.**

## 1. Strategia bezpieczeństwa bazy danych.

### a) **Charakterystyka wycinka świata rzeczywistego**

*Poniżej zamieszczony jest opis dziedziny pochodzący z projektu BZDN_P1, stanowiący charakterystykę kontekstu systemu bezpieczeństwa, który jest przedmiotem niniejszego opracowania. Pominięte zostały natomiast składowe poświęcone modelowaniu bazy danych – wyodrębnione klasy obiektów i powiązania między nimi, a także opis funkcji systemu.*

Wypożyczalnia samochodowa to firma oferująca wynajem samochodów na określony czas. W skład wypożyczalni wchodzą różne kategoria samochodów, takie jak: samochody osobowe, dostawcze oraz specjalistyczne pojazdy, takie jak samochody terenowe czy sportowe, każda kategoria ma przypisaną cenę za jeden dzień wynajmnu.

Obiekty świata rzeczywistego wypożyczalni samochodowej to przede wszystkim samochody, które są najważniejszym produktem oferowanym przez tę firmę. Każdy samochód ma swoje atrybuty, takie jak marka, model, rok produkcji, ilość drzwi, czy wyposażenie dodatkowe jak na przykład: klimatyzacja czy nawigacja.

Innymi obiektami wypożyczalni samochodowej są klienci, którzy wypożyczają samochody. Każdy klient ma swoje dane osobowe, takie jak imię, nazwisko, adres, numer telefonu, adres e-mail. Przy rejestracji nowego klienta należy sprawdzić jego prawo jazdy, aby wiedzieć jakie pojazdy może wypożyczyć, przy jego uprawnieniach.

Procesy zachodzące w wypożyczalni samochodowej to przede wszystkim wypożyczanie samochodów. Klienci składają zamówienie na wynajem samochodu, określając daty wypożyczenia oraz oddania, klient może również wybrać rodzaj ubezpieczenia i usługi dodatkowe jak na przykład: dostarczenie samochodu pod wskazany adres, czy brak konieczności umycia auta przed zwrotem. Każde wypożyczenie ma przypisanego jednego pracownika, który jest odpowiedzialny za jego realizację. Klient odbiera samochód i po określonym czasie zwraca go do wypożyczalni. Samochód zmienia dostępność na niedostępny do czasu zwrotu.

### b) **Grupy użytkowników**, ich sposób korzystania z systemu, zakres i stopień dostępu do danych.

Z systemu korzysta 5 głównych grup użytkowników o zróżnicowanym poziomie dostępu do danych.

- **Klienci** (zarejestrowane osoby, które chcą wypożyczyć samochód) - Klient może dokonać wypożyczenia przez internet lub bezpośrednio w oddziale wypożyczalni. Klient ma dostęp do informacji o samochodach, usługach i ubezpieczeniach wraz z cenami i opisami oraz swojej historii wypożyczeń. Klienci mogą edytować własne dane i usuwać konto (pod warunkiem, że ich historia wypożyczeń jest pusta).
- **Sprzedawcy** (osoby odpowiedzialne za realizację wypożyczenia) - Pracownik może rejestrować klientów, przeglądać historię wypożyczeń oraz generować faktury. Mają uprawnienia do wyświetlania danych wszystkich pracowników, ale bez możliwości edytowania (oprócz swoich

własnych), czy dodawania nowych. Mogą również zmieniać dostępność samochodów, jeżeli system nie zrobi tego automatycznie (np. w przypadku naprawy)

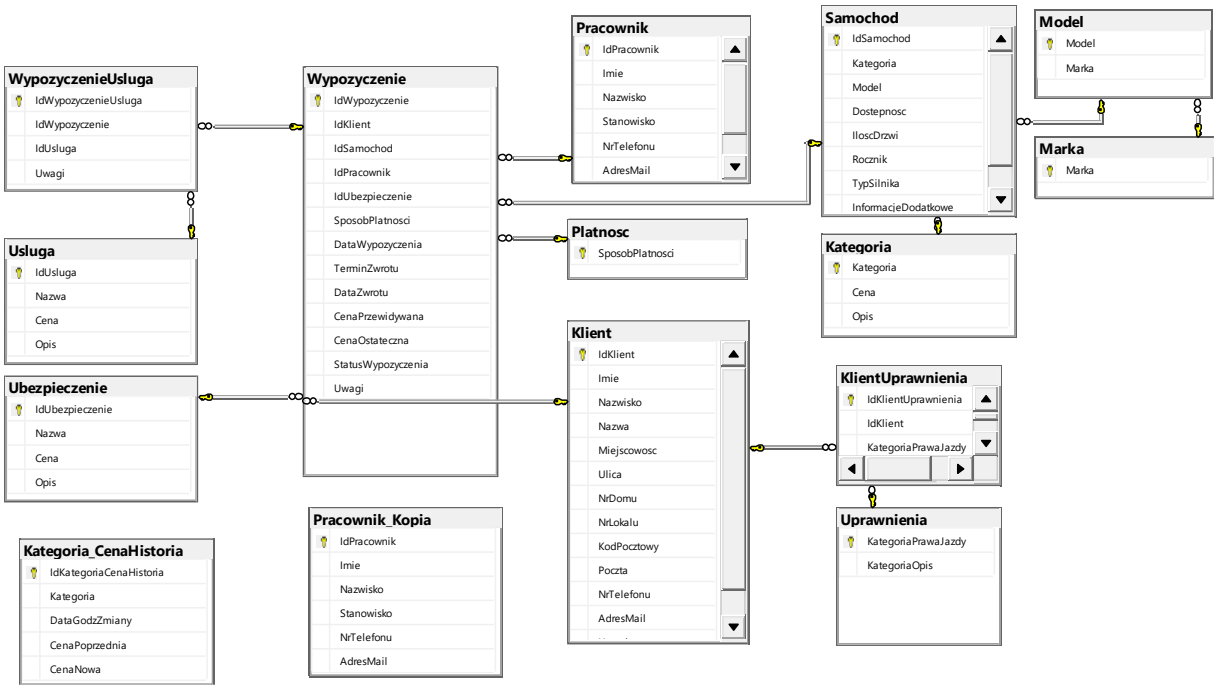
- **Administratorzy** (właściciele firmy, administratorzy systemu informatycznego) – nieograniczone uprawnienia do operowania na danych, w tym modyfikowania słowników.
- **Pracownicy administracyjni** (np. księgowość, kadry i płace) - mają pełne zarządzanie danymi pracowników, a także dostęp do pozostałych tabel, ale tylko w celu ich wyświetlania bez możliwości modyfikowania.
- **Goście** (anonimowi użytkownicy internetowi) - mają możliwość przeglądania oferty wypożyczeń i usług oraz rejestracji w systemie - tworzenia nowego konta klienta.

Szczegółowy opis uprawnień poszczególnych grup użytkowników przedstawiony jest w poniższej macierzy CRUD (ang. create, read, update, delete). Jeżeli określone uprawnienie nie obejmuje całej tabeli, lecz tylko jej część (np. dostęp wyłącznie do własnych danych w profilu użytkownika), fakt ten oznaczony jest symbolem (*).

*Tab. 1 Macierz CRUD - ogólna specyfikacja uprawnień grup użytkowników do tabel bazy danych.*

| | Grupy użytkowników | | | | |
|---|---|---|---|---|---|
| Tabele | Administratorzy | Pracownicy administracyjni | Sprzedawcy | Klienci | Goście |
| *Klient* | C R U D | - R - - | C R U D | - R* U* D* | C* - - - |
| *Pracownik* | C R U D | C R U D | - R* U* - | - R* - - | - - - - |
| *Samochód* | C R U D | - R - - | - R U - | - R - - | - R - - |
| *Kategoria* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *Marka* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *Model* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *Wypożyczenie* | C R U D | - R - - | C R U D | C* R* U* - | - - - - |
| *Usługa* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *Ubezpieczenie* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *Uprawnienia* | C R U D | - R - - | - R - - | - R - - | - R - - |
| *KlientUprawnienia* | C R U D | - R - - | C R U D | C* R* U* - | - - - - |
| *Platnosc* | C R U D | - R - - | - R - - | - R - - | - - - - |
| *WypożyczenieUsługa* | C R U D | - R - - | C R U D | C* R* U* - | - - - - |
| *Kategoria_CenaHistoria* | C R U D | - R - - | C R - - | - - - - | - - - - |
| *Pracownik_Kopia* | C R U D | C R U D | - - - - | - - - - | - - - - |

*Rys. 1 Schemat bazy danych wypożyczalni samochodowej - diagram z programu Microsoft SQL Server Management Studio.*




## c) Założenia strategii bezpieczeństwa

**Z1.** Projektowany system bezpieczeństwa ma na celu zapewnienie przede wszystkim **poufności** (ang. *confidentiality*) danych przechowywanych w bazie poprzez kontolę dostępu do nich – dostosowaną do potrzeb, kompetencji i uprawnień poszczególnych grup użytkowników systemu informatycznego. Nie są tutaj rozpatrywane aspekty integralności (ang. *integrity*) oraz dostępności (ang. *availability*) danych, ani mechanizmy ich szyfrowania – zarówno podczas przechowywania w obrębie struktur bazy, jak i przesyłania poprzez sieć komputerową.

**Z2.** W projekcie przyjęto **zasadę najmniejszych uprawnień** (ang. *principle of least privilege*): określonemu użytkownikowi przyznawane są wyłącznie takie uprawnienia dostępu do bazy danych oraz funkcji systemu, które są niezbędne do wykonywania zadań przewidzianych dla niego w organizacji (czyli tutaj w przykładowej wypożyczalni samochodowej).

**Z3.** Kontrola dostępu do danych i funkcji oparta jest na **rolach** (ang. *roles*) – wspólnych wzorcach uprawnień, które są charakterystyczne dla grup użytkowników o takim samym lub bardzo zbliżonym zakresie obowiązków i kompetencji w organizacji. Nie są natomiast rozpatrywane odrębne uprawnienia pojedynczych użytkowników (ang. *users*), odpowiadających indywidualnym pracownikom, ponieważ skład osobowy firmy jest zależny od konkretnego wdrożenia i może zmieniać się w czasie.

**Z4.** W zewnętrznej, serwerowej warstwie systemu bezpieczeństwa, z wyjątkiem domyślnej roli public kontom logownia (ang. *users*) nie są nadawane żadne role serwerowe (ang. *server roles*), gdyż użytkownicy końcowi nie mają wykonywać operacji konfiguracyjnych w obrębie serwera, a jedynie korzystać z pojedynczej bazy danych.

**Z5.** W warstwie wewnętrznej – na poziomie bazy danych, oprócz domyślnej roli public, użytkownicy nie mają przypisywanych żadnych wbudowanych ról bazodanowych (ang. *fized*

*database roles*), takich jak *db_datareader*, czy *db_datawriter*, ponieważ są one zbyt ogólne względem rozkładu uprawnień wyznaczonego przez macierz CRUD (zob. Tab. 1).

**Z6.** Uprawnienia użytkowników implementowane są w opraciu o **własne role bazodanowe** (ang. *user-defined database roles*), które odpowiadają grupom użytkowników zdefiniowanym w macierzy CRUD (zob. Tab. 1). Przyjmuje się przy tym, że role te są całkowicie rozłączne, to znaczy jeden użytkownik bazy danych może jednocześnie należeć tylko do jednej roli.

**Z7.** Wszystkie **uprawnienia** pozytywne (GRANT) definiowane są wyłącznie **na poziomie obiektów** (ang. *object-level permissions*), nie są zaś nadawane ogólne uprawnienia do wykonywania poleceń (bez dniesienia do obiektów), gdyż ich użycie byłoby nieprzewidywalne i trudne do kontrolowania.

**Z8.** Jeżeli dla jakiejś roli nie jest przewidziany dostęp do pewnego obiektu, jest on jawnie jej zabraniany (DENY), bez pozostawienia uprawnień w stanie nieokreślonym (ani GRANT, ani DENY). Nie jest również stosowane nadpisywanie uprawnień – wielokrotne definiowanie różnych uprawnień do tego samego polecenia lub obiektu (np. najpierw DENY SELECT ON <tabela> TO <rola>, potem GRANT SELECT ON <tabela> TO <rola>).

**Z9.** Na poziomie technicznym wszystkie własne role bazodanowe mają **zabroniony bezpośredni dostęp** (DENY) **do samych tabel**, wymagane zaś operacje na danych realizowane są **wyłącznie za pośrednictwem procedur przechowywanych** (GRANT EXECUTE). Jest to rozwiązanie bezpieczniejsze, a przy tym łatwiejsze do zaimplementowania i późniejszego zarządzania od wariantu opartego na bezpośrednim dostępie do tabel.

**Z10.** Jeżeli użytkownik należący do określonej roli ma uzyskać dostęp tylko do własnych danych (np. swojego profilu klienta lub wykazu swojej historii wypożyczeń), wymagane zawężenie zbioru wierszy realizowane jest przez procedurę przechowywaną, do której – podczas rzeczywistego użycia – muszą zostać przekazane z zewnątrz (np. z poziomu aplikacji) odpowiednie parametry wyznaczające kontekst (np. identyfikator klienta).

### d) **Role bazodanowe i ich uprawnienia – poziom techniczny**

Poniżej wyspecyfikowane są szczegółowe uprawnienia ról bazodanowych do obiektów bazy danych – z uwzględnieniem założeń wymienionych w punkcie (c). Dostęp wymagający dostępu kontekstu użycia (np. klient może przeglądać i modyfikować wyłącznie swoje dane) oznaczony jest symbolem (*).

*Tab. 2 Techniczna specyfikacja uprawnień ról bazodanowych do obiektów bazy danych: tabel (T) oraz procedur (P).*

| | Role bazodanowe | | | | |
|---|---|---|---|---|---|
| Obiekty bazy danych | *Administratorzy* | *PracownicyAdm* | *Sprzedawcy* | *Klienci* | *Goscie* |
| *dbo.Kategoria* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Kategoria_CenaHistoria* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Klient* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.KlientUprawnienia* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Marka* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Model* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Platnosc* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Pracownik* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Pracownik_Kopia* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |

| | | | | | |
|---|---|---|---|---|---|
| *dbo.Samochod* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Ubezpieczenie* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Uprawnienia* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Usluga* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Wypozyczenie* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.WypozyczenieUsluga* (T) | - - - - | - - - - | - - - - | - - - - | - - - - |
| *dbo.Kategoria_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Kategoria_Usun* (P) | E | - | - | - | - |
| *dbo.Kategoria_Wstaw* (P) | E | - | - | - | - |
| *dbo.Kategoria_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Kategoria_ZmienCene* (P) | E | - | E | - | - |
| *dbo.Kategoria_Znajdz_Cena* (P) | E | E | E | E | E |
| *dbo.Klienci_Wypozyczenia* (P) | E | - | E | - | - |
| *dbo.Klient_CenaWypozyczenia* (P) | E | - | E | - | - |
| *dbo.Klient_Miejscowosci* (P) | E | - | E | - | - |
| *dbo.Klient_Modyfikuj* (P) | E | - | E | E* | - |
| *dbo.Klient_Szukaj* (P) | E | E | E | - | - |
| *dbo.Klient_Usun* (P) | E | - | E | E* | - |
| *dbo.Klient_Wstaw* (P) | E | - | E | - | E* |
| *dbo.Klient_Znajdz_Id* (P) | E | E | E | E* | - |
| *dbo.Klient_Znajdz_Nazwisko* (P) | E | E | E | - | - |
| *dbo.Klient_Znajdz_Wzorzec* (P) | E | E | E | - | - |
| *dbo.KlientUprawnienia_Modyfikuj* (P) | E | - | E | E* | - |
| *dbo.KlientUprawnienia_Usun* (P) | E | - | E | - | - |
| *dbo.KlientUprawnienia_Wstaw* (P) | E | - | E | E* | - |
| *dbo.KlientUprawnienia_Wyswietl* (P) | E | E | E | E* | - |
| *dbo.Marki_Popularnosc* (P) | E | - | E | - | - |
| *dbo.Marka_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Marka_Usun* (P) | E | - | - | - | - |
| *dbo.Marka_Wstaw* (P) | E | - | - | - | - |
| *dbo.Marka_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Model_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Model_Usun* (P) | E | - | - | - | - |
| *dbo.Model_Wstaw* (P) | E | - | - | - | - |
| *dbo.Platnosc_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Platnosc_Usun* (P) | E | - | - | - | - |
| *dbo.Platnosc_Wstaw* (P) | E | - | - | - | - |
| *dbo.Platnosc_Wyswietl* (P) | E | E | E | E | - |
| *dbo.Model_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Pracownicy_Ranking* (P) | E | E | - | - | - |
| *dbo.Pracownik_Archiwizuj* (P) | E | E | - | - | - |
| *dbo.Pracownik_Modyfikuj* (P) | E | E | E* | - | - |
| *dbo.Pracownik_Usun* (P) | E | E | - | - | - |
| *dbo.Pracownik_Wstaw* (P) | E | E | - | - | - |
| *dbo.Pracownik_Znajdz_Id* (P) | E | E | E* | - | - |
| *dbo.Pracownik_Znajdz_Nazwisko* (P) | E | E | - | - | - |
| *dbo.Samochod_Dostepnosc* (P) | E | E | E | E | E |
| *dbo.Samochod_Modyfikuj* (P) | E | - | E | - | - |
| *dbo.Samochod_Usun* (P) | E | - | - | - | - |
| *dbo.Samochod_Wstaw* (P) | E | - | - | - | - |

| | | | | | |
|---|---|---|---|---|---|
| *dbo.Samochod_Wstaw_Makro* (P) | E | - | - | - | - |
| *dbo.Samochody_Marki* (P) | E | - | E | - | - |
| *dbo.Ubezpieczenie_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Ubezpieczenie_Usun* (P) | E | - | - | - | - |
| *dbo.Ubezpieczenie_Wstaw* (P) | E | - | - | - | - |
| *dbo.Ubezpieczenie_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Uprawnienia_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Uprawnienia_Usun* (P) | E | - | - | - | - |
| *dbo.Uprawnienia_Wstaw* (P) | E | - | - | - | - |
| *dbo.Uprawnienia_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Usluga_Modyfikuj* (P) | E | - | - | - | - |
| *dbo.Usluga_Niedodawane* (P) | E | - | E | - | - |
| *dbo.Usluga_Usun* (P) | E | - | - | - | - |
| *dbo.Usługa_Wstaw* (P) | E | - | - | - | - |
| *dbo.Usluga_Wyswietl* (P) | E | E | E | E | E |
| *dbo.Wypozyczenie_Aktualne* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Modyfikuj* (P) | E | - | E | E* | - |
| *dbo.Wypozyczenie_N_OstatnichDni* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Szukaj_Okres* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Usun* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Wstaw* (P) | E | - | E | E* | - |
| *dbo.Wypozyczenie_Zestawienie* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Znajdz_Daty* (P) | E | - | E | - | - |
| *dbo.Wypozyczenie_Wyswietl* (P) | E | E | E | E* | - |
| *dbo.WypozyczenieUsluga_Modyfikuj* (P) | E | - | E | E* | - |
| *dbo.WypozyczenieUsluga_Usun* (P) | E | - | E | - | - |
| *dbo.WypozyczenieUsluga_Wstaw* (P) | E | - | E | E* | - |
| *dbo.WypozyczenieUsluga_Wyswietl* (P) | E | E | E | E* | - |

### e) **Imprementacja i testowanie mechanizmów bezpieczeństwa**

Role bazodanowe oraz ich uprawnienia zostały zaimplementowane w skrypcie T-SQL: **S19_P1_uprawnienia.sql**.

Polecenia służące do weryfikacji działania oprogramowanych mechanizmów, wyniki testowania oraz obserwacje i wnioski z nich płynące – zawarte są w pliku: **S19_P1_testowanie.sql**.