УДК 004.415.2
В. Нагаєнко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА СУЧАСНИХ МЕТОДІВ ТА АЛГОРИТМІВ АВТЕНТИФІКАЦІЇ МОДУЛЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ

UDC 004.415.2
V. Nahaienko, st.

DEVELOPMENT OF A METHOD FOR DELIMITING ACCESS TO DATA

Основна мета проекту – розробити інформаційну систему для управління компаніями із розмежуванням доступу до даних. Дана робота включає розробку програмного забезпечення на основі використання баз даних.

З допомогою модуля доступу можна регулювати права до функціональних можливостей системи та перегляду інформації для конкретного користувача та групи користувачів.

Модуль розмежування доступу дозволяє організувати використання різних модулів системи відповідно до встановлених для певного користувача прав.

В якості технологій було обрано ASP.NET Core та СУБД MSSQL. Середовищем розробки була обрана Microsoft Visual Studio, SQL Server Management Studio. Для програмної системи була обрана мова C#. При роботі з базою даних було використано збережені процедури, функції, представлення.

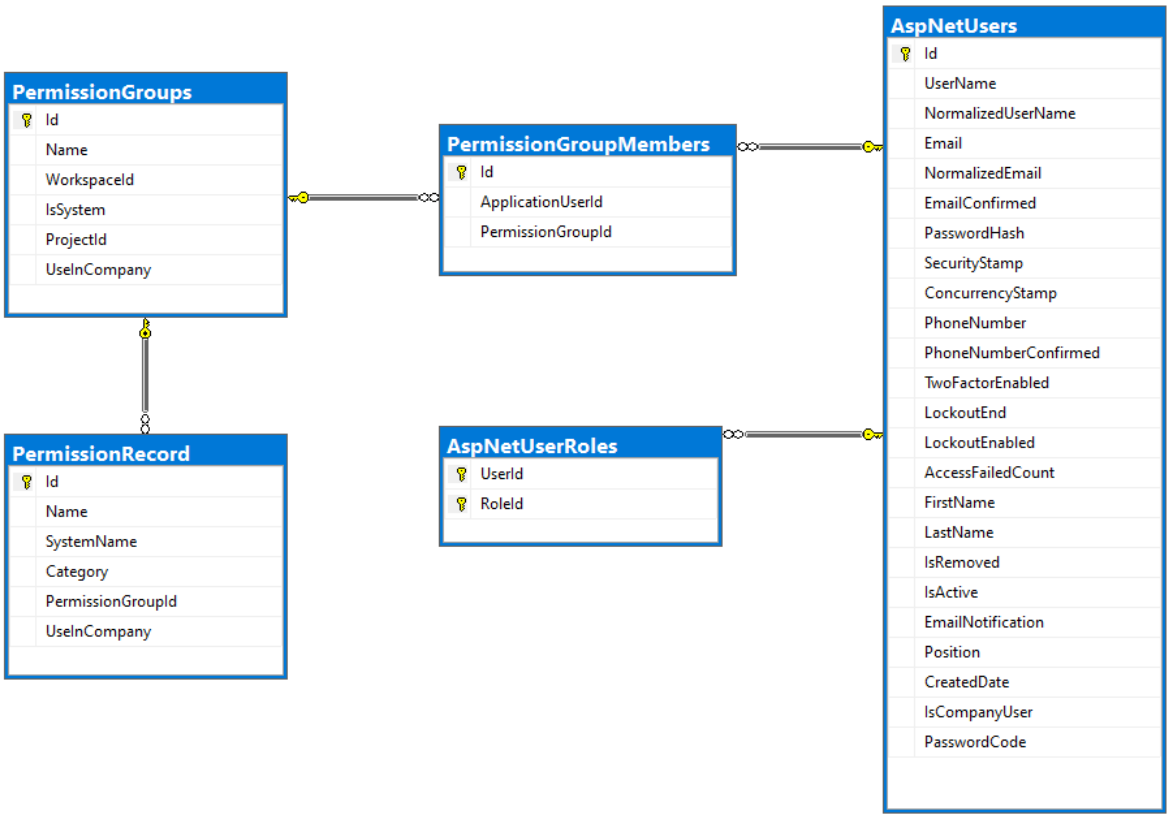

Рисунок 1. Діаграма таблиць бази даних для розмежування доступу

В якості предметної області обрано систему для внутрішнього менеджменту компаній, в якості розмежування доступу до тих чи інших функцій або даних використано два підходи – на основі ролей та на основі пермішинів.

Для менеджменту всіма компаніями зі сторони системи призначається спеціальний працівник якому надається роль CompanyAdmin адміністратором системи, тобто користувачем з ролью SystemAdmin, другий підхід передбачає використання пермішинів які надає власник компанії.

Ролі діють глобально на всю систему і призначаються виключно адміністратором, тоді як пермішини діють локально в рамках компаній і можуть придумуватись будь-які в залежності від вибраних комбінацій прав власником або членом компанії з потрібними для цього пермішинами.

Для передачі даних про права користувача при авторизації повертається токен з закодованими ролями і пермішинами для надання доступу до частин системи, токен розкодовується і обробляється на клієнті а також на сервері при відправленні запитів. Аутентифікація і авторизація в системі реалізована основі JWT токенів протоколу OAuth2 та є досить надійною оскільки використовуються Access та Refresh токени, тому у випадку викрадення токена з певними правами шкоду можна звести до мінімуму.

Література.

1. SQL Server 2019 Administration Inside Out 1st Edition (Randolph West, Melody Zacharias, William Assaf, Sven Aelterman, Louis Davidson, Joseph D’Antoni).
2. The Data Access Handbook: Achieving Optimal Database Application Performance and Scalability 1st Edition (John Goodson, Robert A. Steward).
3. Big Data and Global Trade Law (Florent Thouvenin and Aurelia Tamò-Larrieux).
4. https://oauth.net/2/
5. https://identityserver4.readthedocs.io/en/latest/