Лабораторна робота №6

1. Реалізація сховищ
   Безпека сховища забезпечується збереженням AEAD зашифрованих персональних даних окремо від ключів, якими ці дані було зашифровано. Ключі зберігаються в зашифрованому вигляді. Ключі шифруються за допомогою головного ключа, який зберігається в AWS KMS сервісі. При кожній зміні даних оновлюється ключ для шифрування цих даних, таким чином розв'язується проблема ротації ключів. Шифрування даних відбувається алгоритмом AES-256-GCM. Кожне поле в таблиці з персональними даними шифрується окремо та до кожного поля зберігається його nonce та auth tag. Дані кожного користувача шифруються іншим ключем. Перед тим, як оновити дані користувач проходить процес авторизації та автентифікації.

2. Для збереження головного ключа було використано AWS KMS сервіс, так як він є визнаним в світі сервісом для зберігання ключів та відповідає всім вимогам системи керування ключами. При шифруванні ключів головним ключем сервіс використовує алгоритм AES-GCM. Цей ж алгоритм використовується нами для шифрування ключами, тому що цей алгоритм забезпечує стійке AEAD шифрування. Шифрування відбувається за допомогою вбудованого в node js модуля crypto без використання сторонніх бібліотек.

3. Інформація може бути вкраденою у випадку, якщо зловмисник отримає доступ до бази даних з персональними даними, до бази даних з DEK та до KEK, який зберігається в сервісі AWS. Зробити всі ці 3 речі непомітно за умови правильного керування паролями та доступами дуже складно.