**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «Київський політехнічний інститут імені Ігоря Сікорського» Факультет інформатики та**

**обчислювальної техніки**

**Кафедра технічної кібернетики**

***Звіт до комп’ютерного практикуму з кредитного модуля* «Security»**

**Лабораторна робота 5**

Виконали

Студенти групи ІТ-84

Лисенко Олег

Бурдейний Володимир

**Київ 2021**

**Завдання**

Для виконання завдання лабораторної роботи було створенно простий веб-сервер за допомогою стандартних можливойстей мови програмування Golang. Була реалізована частина з реєстрацією на сайті, де користувач вводить свої дані та пароль. Пароль хешується на стороні сервера за допомогою алгоритму bcrypt з десятикратним циклом “соління”. Результуючий хеш зберігається в базу даних. В якості бази даних була обрана не реляційна MongoDB.

Для хешування була обрана реалізації bcrypt зі стандартного набору функцій мови golang.

hash, err := bcrypt.GenerateFromPassword([]byte(newUser.Password), 10)

Для валідації пароля при вході користувача в систему використовується наступна функція.

bcrypt.CompareHashAndPassword(pwd, []byte(loggingUser.Password))

До форми самого пароля є також вимоги — він повинен бути як найменше 8 символів в довжину, містити цифри та літери нижнього й верхнього регістрів.

**Висновок**

У ході виконання лабораторної роботи ми ознайомили з найкращими практиками для зберігання паролів та їх подальшої валідації. Нами було розроблено та на прикладі перевірено практичність такого підходу. Працюючи над цією роботою ми отрмали навичи практичного використання алгоритмів хешування.