**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 6**

Виконали

Студенти групи ІТ-84

Лисенко Олег

Бурдейний Володимир

**Київ 2021**

**Завдання**

Дана лабораторна робота була виконано на основі 5 лабораторної роботи. Для вебсервера використоні стандартні засоби мови golang. В якості бази даних була обрана не реляційна MongoDB.

Дані, які вводить користувач про себе зберігаються у базі данних в зашифрованому вигляді. В якості алгоритму шифрування був обран алгоритм

aes-256-gcm. Шифри зберігаються у базі даних, а колючі від них у файловій системі з обмеженим доступом до них.

Шифрування відбувається наступним чином

key, err := hex.DecodeString(keyStr)  
if err != nil {  
 return "", err  
}  
block, err := aes.NewCipher(key)  
if err != nil {  
 return "", err  
}  
aesGcm, err := cipher.NewGCM(block)  
if err != nil {  
 return "", err  
}  
nonce := make([]byte, aesGcm.NonceSize())  
if \_, err = io.ReadFull(rand.Reader, nonce); err != nil {  
 return "", err  
}  
enc := aesGcm.Seal(nonce, nonce, []byte(data), nil)

**Висновок**

У ході виконання лабораторної роботи ми ознайомили з найкращими практиками для шифрування даних. Нами було розроблено та на прикладі перевірено практичність такого підходу. Працюючи над цією роботою ми отрмали навичи практичного використання алгоритмів шифрування.