

**ПРАКТИЧНА РОБОТА 07**  
**Забезпечення безпеки в операційних системах**  
**Система оцінювання**

№	Тема	К-ть балів
1.	<i>Захист принаймні одного завдання з роботи</i>	1
2.	Практичні завдання	3,6*
3.	<i>Здача звіту</i>	0,4
	<b>Всього</b>	<b>5</b>

\* – діє бонусна система

1. *1,6 бала* Реалізуйте безпечну передачу трафіку в TCP-тунелі, використовуючи *власну* реалізацію алгоритму Advanced Encryption Standard (AES-128). Для прикладу можете розглянути [реалізацію](#) мовою Python на основі бібліотеки PyCrypto.
2. *0,8 бала* Розробіть програмне забезпечення для автентифікації користувача, використовуючи хешування паролю відповідно до хеш-функції згідно з Вашим варіантом:

№	Хеш-функція	Сіль
1	SHA-256	ytggy345bfs
2	SHA-1	p3o4fre7fg4
3	SHA-384	nbvr5o64e11
4	SHA-512	87934fdghcx
5	MD5	63gfaq5qqq5
6	SHA-224	mbcygffd093
7	SHA-256	fdf34jv0bwe
8	SHA-1	ooptet56ghs
9	SHA-384	bvcrt7gg6f
10	SHA-512	7kk8re2vcxz
11	MD5	09tgfio63gdm
12	SHA-224	m823fsdjzza
13	SHA-256	zxcvbnm0111
14	SHA-1	987654321gtv
15	SHA-384	memoopcqp2
16	SHA-512	lkwevbtttd30
17	MD5	aaaaaaaaaaaa
18	SHA-224	zcdpok65w2

Базу даних з паролями можете зберігати у вигляді текстового файлу. Окремо постачайте конфігураційний файл, який міститиме сіль. При реалізації мовою Python рекомендується використовувати бібліотеку hashlib. Доповніть зміст вище згаданими файлами.

3. **(Завдання для всіх)** <sup>1,2 бала</sup> Виконайте хешування MAC-адреси свого комп'ютера за допомогою алгоритму MD5 та створіть зведену таблицю з хешами для груп. Оберіть один з методів отримання MAC-адреси за допомогою мови Python. Реалізуйте [клієнт-серверне](#) програмне забезпечення, яке триматиме на «сервері» скрипт з фільтруванням MAC-адрес по групах. Наприклад, при доречності MAC-адреси для своєї групи, буде виводитись повідомлення про перехід у зону групи. Але при зверненні в зону чужої групи доступ буде заблоковано (виведено спеціальне повідомлення). Можливо, забажаєте спробувати створити [простий веб-сервер](#).