Лабораторні роботи № 3.

Тема. Апаратні засоби захисту інформації в комп'ютерних системах.

Мета. Формування знань класифікації, призначення, особливостей застосування апаратних засобів захисту інформації в комп'ютерних системах. Систематизація знань файлової структури, вмінь і навиків використання текстових процесорів та засобів захисту текстових документів.

Підготовчий етап заняття. Актуалізація знань

1. В друкованих джерелах та Інтернеті віднайдіть інформацію про різновид апаратного засобу захисту чи зламу захисту інформації в комп'ютерних системах згідно варіанта:

№ варіанта	Апаратний засіб
1.	Апаратні ключі на основі Flash-пам'яті.
2.	Апаратні ключі на основі чіпів.
3.	„Ключові" диски.
4.	СМАРТ-карти.
5.	Плати контролю циклу завантаження.
6.	Захисні засоби знищення конфіденційної інформації на накопичувачах.
7.	Плати для шифрування.
8.	TCG (TPM)-чіпи.
9.	Системи електромагнітного зашумлення.
10.	Високочастотні фільтри на лініях зв'язку.
11.	Детектори прихованих відеокамер.
12.	Детектори підслуховуючих пристроїв.
13.	Детектори GSM та Bluetooth.
14.	Плати відеозахоплення.
15.	Відеокамери з можливістю віддаленого управління.
16.	Клавіатурні зчитувачі.
17.	Бездротові радіомікрофони.
18.	Перехоплювачі електромагнітних випромінювань.

Формування опису різновиду апаратного засобу захисту чи зламу захисту

1. У текстовому процесорі *MS Word 2010* опишіть різновид апаратного засобу захисту чи зламу захисту (**0.8 – 1 сторінка**) з віднайдених вами джерел за планом (**пункти плану наводяться у тексті з зазначенням конкретного апаратного засобу**):

№	Пункт плану
1.	Призначення апаратного засобу захисту чи зламу захисту.
2.	Зовнішній вигляд (форма реалізації) апаратного засобу.
3.	Послідовність встановлення апаратного засобу.
4.	Принципи реалізації захисту чи зламу захисту.
5.	Принципи зламу захисту чи механізми виявлення апаратного засобу захисту.
6.	Висновки про переваги, недоліки та перспективи розвитку і поширення апаратного засобу.

2. Збережіть створений опис апаратного засобу у файлі-звіті, ім'я якого має містити шифр групи (наприклад, ЕК51) та прізвище виконавця без пробілів.
3. Розмістіть у тексті звіту під заголовком у верхньому лівому кутку якісне зображення апаратного засобу розміром 4 х 5 см. з обтіканням його текстом по контуру.
4. Встановіть для файла звіту:
   - поля: верхнє та нижнє – по 2 см, ліве та праве – по 1 см, переплетення – 1 см.;
   - відступи від краю до колонтитула – по 1 см.;
   - міжрядковий інтервал – одинарний.
5. Відформатуйте текст звіту, забезпечивши:
   5.1. Для основного тексту:
   - назва стилю – *Обычный*;
   - шрифт тексту – *Times New Roman*;
   - розмір шрифта – *12 пунктів*;
   - орієнтація тексту абзацу – *по ширині*;
   - відступ першого рядка абзацу – *1.25 см*.

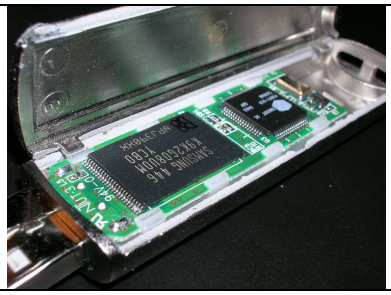
   5.2. Для заголовків пунктів плану:
   - назва стилю – *Заголовок3*;
   - розмір шрифта – *14 пунктів*;
   - орієнтація тексту абзацу – *по центру*;
   - відступ першого рядка абзацу – 0 см.
6. В кінці звіту подайте список використаних джерел за діючими стандартами бібліографічного опису. Створіть у тексті на номери у цьому списку автоматичні посилання.

Завершальний етап заняття

7. Створіть електронний лист у своїй поштовій скриньці на сайті gmail.com. Приєднайте до цього листа створений документ. Тему листа сформуйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *ЕК51_ЛР3_Величко Володимир*. Надішліть створений лист на адресу LRZaxInf@gmail.com.
8. Збережіть створений документ на власному носії, адже він знадобиться вам при виконанні наступної лабораторної роботи.

Критерії оцінювання звіту.

1. Відповідність тексту заданому плану.
2. Відповідність форматування наведеним вимогам.
3. Цілісність викладу матеріалу.
4. Наявність автоматичних посилань на джерела.
5. Вчасність пересилання файла звіту.

Апаратні ключі на основі Flash-пам’яті.	
Апаратні ключі на основі чіпів.	
„Ключові” диски.	
CMAPT-карти.	
Плати контролю циклу завантаження.	
Захисні засоби знищення конфіденційної інформації на накопичувачах.	
Плати для шифрування.	
TCG (TPM)-чіпи.	
Системи електромагнітного зашумлення.	
Високочастотні фільтри на лініях зв’язку.	
Детектори прихованих відеокамер.	
Детектори підслуховуючих пристроїв.	
Детектори GSM та Bluetooth.	
Плати відеозахоплення.	
Відеокамери з можливістю віддаленого управління.	
Клавіатурні зчитувачі.	
Бездротові радіомікрофони.	
Перехоплювачі електромагнітних випромінювань.	