ПРОГРАМОВІ ВИМОГИ З ДИСЦИПЛІНИ «ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ»

Тема1. Складові "Інформаційної безпеки".

1.1 Поняття інтелектуальної власності.
1.2 Важливість захисту програмного забезпечення в сучасних умовах.
1.3 Література, методичні рекомендації щодо дисципліни.

Тема 2. Огляд метолів та засобів захисту інформації.

2.1 Причини існування комп'ютерних злодіїв.
2.2 Методи проникнення до інформації у комп'ютері (хакінг, крекінг, фрікінг).
2.3 Класифікація методів та засобів захисту програмного забезпечення.
2.4 Апаратні, програмні та програмно-апаратні засоби захисту інформації.
2.5 Носії ключової інформації (дискети, електронні ключі, SMART-карти, пристрої Touch-Memory).
2.6 Прив'язка програмного забезпечення до унікальних характеристик комп'ютерної системи та BIOS.

Тема 3. Система захисту компютера з допомогою BIOS.

3.1 Основні складові програми BIOS.
3.2 Принципи хешірования та зберігання паролів доступу.
3.3 Інженерний пароль, старий та новий формат паролю, місце зберігання інженерного паролю в BIOS.
3.4 Програмний пароль, місце знаходження програмних паролів (SUPERVISOR та USER) в CMOS-пам'яті.

Тема 4. Методи захисту програмних продуктів.

4.1 Засоби аналізу парольного хеша.
4.2 Методи зняття, взлому та підбору паролю.
4.3 Програмні засоби хакерів для зняття та взлому паролю BIOS.
4.4 Рекомендації щодо унеможливлення несанкціонованого доступу до комп'ютеру.

Тема5. Побудова системи безпеки ОС WINDOWS 2k.

5.1 Файлова система NTFS, її роль у захисті інформації.
5.2 Принципи адміністрування у ОС WINDOWS 2k.
5.3 Створення системи облікових записів.

Тема 6. Побудова системи безпеки ОС UNIX.

6.1 Особливості функціонування ОС UNIX.
6.2 Система доступу та реєстрації користувачів у ОС UNIX та LINUX.
6.3 Базові консольні команди *NIX та система каталогів.

Тема 7. Методи протидії штучно занесеним руйнівним комп'ютерним програмам.

7.1 Класифікація засобів, що використовують при зломі програм.
7.2 Методи аналізу програм із допомогою HEX-редакторів, дизасемблерів та відладчиків.
7.3 Послідовність дій при зломі програмного продукту.
7.4 Виготовлення CRACK-файлів.

Тема 8. Програмні засоби підвищення рівня захисту.

8.1 Прийоми захисту програм шляхом динамічного генерування програмного коду.
8.2 Ускладнення дизасемблювання програм шляхом використання самомодіфікуючогося коду.
8.3 Методи виявлення роботи програми під відладчиком.