**Міністерство освіти та науки України**

**Державний торговельно-економічний університет**

***Кафедра інженерії програмного забезпечення та кібербезпеки***

**ЗВІТ**

***З ЛАБОРАТОРНОЇ РОБОТИ № 6***

*з дисципліни*

**«ОСНОВИ КІБЕРБЕЗПЕКИ»**

**НА ТЕМУ:**

КОМП’ЮТЕРНІ ВІРУСИ: ЗНАЙОМСТВО З ПРИНЦИПАМИ РОБОТИ. ЗАХИСТ ВІД ВІРУСІВ. ОГЛЯД ОСНОВНИХ АНТИВІРУСНИХ ПРОГРАМ

(назва теми)

**Виконала:** студентка факультету інформаційних технологій

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Ковальова Людмила Ігорівна

Київ 2024

**Лабораторна робота №6**

**Тема**: комп’ютерні віруси: знайомство з принципами роботи. Захист від вірусів. Огляд основних антивірусних програм

**Мета**: ознайомитись з основними видами комп’ютерних вірусів, принципами їх роботи поширення і знищення. Розглянути програми для захисту від вірусів, принцип дії, ефективність, можливості.

**Хід роботи:**

Завантажувальні віруси

1. Назви вірусів даного типу:
   1. Stoned
   2. Michelangelo
   3. Form
   4. CIH (Chernobyl)
   5. Brain
   6. Stoned Angelina
   7. Stealth
   8. Monkey
   9. Angelina
2. Принцип роботи:

Вірус вбудовується в сектор завантаження і активується при кожному запуску комп'ютера або пристрою.

Після запуску вірус може перехоплювати процес завантаження операційної системи, завантажуючи спеціальний код в пам'ять.

1. Методи поширення:
   1. Збудження на комп'ютер або пристрій зараженого додатку або оперативної системи.
   2. Передача через заражені дискети, USB-накопичувачі або інші носії.
2. Алгоритм роботи вірусу:
   1. Завантаження вірусу в пам'ять системи під час процесу завантаження.
   2. Перехоплення процесу завантаження і виконання шкідливого коду.
   3. Пошук нових носіїв для поширення.
3. Методи знищення:
   1. Використання антивірусних програм для виявлення та видалення вірусу.
   2. Перезаписання або відновлення сектора завантаження з джерела безпечного диска або іншого носія.
4. Програми для знищення:
   1. Zillya!
   2. McAfee Antivirus
   3. Norton Antivirus
   4. Bitdefender Antivirus
   5. AVG Antivirus
5. Методи знищення:
   1. Сканування комп'ютера або пристрою з використанням антивірусних програм для виявлення та видалення вірусу.
   2. Перезаписання або відновлення сектора завантаження за допомогою спеціальних утиліт або команд відновлення операційної системи.

**Висновок:** в ході виконання лабораторної роботи було вивчено принципи роботи комп’ютерних вірусів, захист від них та огляд основних антивірусних програм. Одним з небезпечних комп’ютерних вірусів є завантажувальний вірус. Вони представляють серйозну загрозу для безпеки інформації, оскільки вони можуть впливати на сектор завантаження пристрою і виконувати свій шкідливий код при кожному запуску системи. Для боротьби з завантажувальними вірусами важливо використовувати надійне антивірусне програмне забезпечення, яке здатне виявляти і видаляти ці віруси, а також використовувати методи відновлення системи до безпечного стану, такі як відновлення сектора завантаження.