**Міністерство освіти і науки України**

**Національний технічний університет України**

**«Київський політехнічний інститУТ»**

**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

**Кафедра математичних методів інформації**

«На правах рукопису» **До захисту допущено**

УДК**\_\_\_\_\_\_\_\_\_\_\_ Завідувач кафедри**

\_\_\_\_\_\_\_\_\_\_ М.М.Савчук

(підпис) (ініціали, прізвище)

“\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_2013р.

МАГІСТЕРСЬКА ДИСЕРТАЦІЯ

з спеціальності 8.04030101 «Прикладна математика»

на тему: Дослідження кубічних атак з малими степенями макстермів\_\_\_\_\_\_\_\_\_

**Студент групи** ФІ-72 Сергієнко Віталій Борисович

(шифр групи) (прізвище, ім’я, по батькові) (підпис)

**Науковий керівник** канд.ф.-м.н., доц. Завадська Л.О.

(вчені ступінь та звання, прізвище, ініціали) (підпис)

**Консультанти:**

### Охорона праці та безпека в НС ст.вик. Чернушак І.І. \_\_\_\_\_\_\_\_\_\_\_

(назва розділу ДП (ДР)) (вчені ступінь та звання, прізвище, ініціали) (підпис)

### 

(назва розділу ДП (ДР)) (вчені ступінь та звання, прізвище, ініціали) (підпис)

**Київ – 2013**

**Національний технічний університет України**

**“Київський політехнічний інститут”**

Факультет (інститут) Фізико - технічний інститут

Кафедра математичних методів захисту інформації

Спеціальність 8.04030101 «Прикладна математика»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_ М.М.Савчук

(підпис) (ініціали, прізвище)

“\_\_\_”\_\_\_\_\_\_\_\_\_\_\_2013р.

**ЗАВДАННЯ**

**на магістерську дисертацію**

студенту \_\_\_\_\_\_\_\_\_\_\_\_Сергієнку Віталію Борисовичу\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище, ім’я, по батькові)

1. **Тема дисертації** Дослідження кубічних атак з малими степенями макстермів

затверджена наказом по університету від “\_\_\_”\_\_\_\_\_\_\_\_ 2013р. №\_\_\_\_\_

2. **Термін здачі** студентом закінченої дисертації “\_\_\_”\_\_\_\_\_\_20\_р.

3. **Об’єкт дослідження**  кубічні атаки з малими степенями макстермів на криптосистеми з наявними відкритими змінними\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. **Предмет дослідження**

аналіз кількості сприятливих функцій та оцінка успішності кубічної атаки з малими степенями макстермів

1. **Перелік питань, які мають бути розроблені**

1) встановити залежність та вивести математичне співвідношення для кількості сприятливих функцій для кубічної атаки з макстермами першого степеня від степеня функції та кількості змінних;

2) перевірити правильність отриманих теоретичних результатів за допомогою програмної реалізації підрахунку кількості сприятливих функцій;

3) оцінити імовірність успіху атаки з малими степенями макстермів в залежності від кількості змінних.

6. **Перелік публікацій**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**7. Перелік ілюстрованого матеріалу**

Рисунок 1.1 – схема гіпотетичного шифру, на який може бути застосована кубічна атака;

рисунки 2.1-2.2 – графіки залежності часової складності кубічної атаки від максимального степеня макстерма та кількості тактів роботи шифру;

рисунок 3.1 – схема програмної реалізації алгоритму перебору і підрахунку кількості сприятливих функцій;

рисунок 4.1 – загальний план приміщення та розташування обладнання;

рисунки 4.2-4.4 – розподіл ізоліній в приміщенні для різних варіантів освітлення;

рисунок 4.5 – план евакуації з приміщення.

**8.Консультанти:**

з питань ОП та БНС \_\_\_\_\_\_\_\_\_\_\_\_ ст.вик. Чернушак І.І.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(вчене звання, ПІБ, посада)

9. **Дата видачі завдання** “\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2011р.

**Науковий керівник** \_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_Л.О. Завадська\_\_\_\_\_\_\_\_

(підпис) (ініціали, прізвище)

**Завдання прийняв до виконання** \_\_\_\_\_\_\_\_\_\_\_\_\_В.Б. Сергієнко\_\_\_

(підпис) (ініціали, прізвище)