Харківський національний університет радіоелектроніки
(повне найменування вищого навчального закладу)

Факультет Комп'ютерної інженерії та управління
(повне найменування інституту, назва факультету (відділення))

Кафедра Безпеки інформаційних технологій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до магістерської атестаційної роботи
Магістр
(освітньо-кваліфікаційний рівень)

на тему: Аналіз криптографічних властивостей перспективних симетричних перетворень

Виконав: студент 5 курсу, групи
БІКСм-12-1
напряму підготовки (спеціальності)
8.17010101, Безпека інформаційних та комунікаційних систем
(шифр і назва напряму підготовки, спеціальності)

Кіянчук Р. І.
(прізвище та ініціали)
Керівник Олійников Р. В.
(прізвище та ініціали)
Рецензент Сватовський І. І.
(прізвище та ініціали)

Харків - 2013 року

Харківський національний університет радіоелектроніки
(повне найменування вищого навчального закладу)

Інститут, факультет, відділення Комп'ютерної інженерії та управління
Кафедра, циклова комісія Безпеки інформаційних технологій
Освітньо-кваліфікаційний рівень Магістр
Напрям підготовки 1701 Безпека інформаційних та комунікаційних систем
(шифр і назва)
Спеціальність 8.17010101 Безпека інформаційних та комунікаційних систем
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри,
голова циклової комісії БІТ
д.т.н., проф. І.Д. Горбенко
"____"_____2013року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ АТЕСТАЦІЙНУ РОБОТУ СТУДЕНТУ

Кіянчуку Руслану Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема магістерської атестаційної роботи: «Аналіз криптографічних властивостей перспективних симетричних перетворень»
керівник магістерської атестаційної роботи
Олійников Роман Васильович, д. т. н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "16"травня 2013 року № 577 СТ.
2. Строк подання студентом магістерської атестаційної роботи
"07" червня 2013 року
3. Вихідні дані до магістерської атестаційної роботи: Специфікації та матеріли з аналізу досліджуваних шифрів (ГОСТ 28147-89, MISTY1).
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

Вступ.
1 Аналіз та синтез сучасних симетричних криптографічних перетворень.
2 Алгебраїчний аналіз симетричних блочних шифрів.
3 Алгебраїчний криптоаналіз шифрів ГОСТ 28147-89 та MISTY1.
4 Опис програмної реалізації розроблених методів.
5 Охорона праці та безпека в надзвичайних ситуаціях.
Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
презентаційні матеріали, представлені слайдами.

6. Консультанти розділів магістерської атестаційної роботи.

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3, 4	Олійников Р. В., проф.		
5	Сердюк Н. М., асист.		

7.Дата видачі завдання 15.03.2013 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської атестаційної роботи	Строк виконання етапів магістерської атестаційної роботи	Примітка
1	Аналіз предметної області, збір та обробка інформації.	15.03 – 31.03	Виконано
2	Дослідження оптимальних методів побудови нелінійних рівнянь для криптографічних перетворень.	01.04 – 20.04	Виконано
3	Реалізація системи нелінійних рівнянь для шифрів ГОСТ 28147-89 та MISTY1.	21.04 – 05.05	Виконано
4	Виконання завдання з розділу «Охорона праці та безпека в надзвичайних ситуаціях».	06.05 – 10.05	Виконано
5	Програмна реалізація та дослідження властивостей алгебраїчної атаки.	11.05 – 15.05	Виконано
6	Аналіз отриманих результатів.	16.05 – 20.05	Виконано
7	Оформлення пояснювальної записки.	21.05 – 1.05	Виконано

Студент _____ Кіянчук Р. І. _____
(підпис) (прізвище та ініціали)

Керівник магістерської атестаційної роботи _____ Олійников Р. В.
(підпис) (прізвище та ініціали)