

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: Дослідження методів формування нелінійних вузлів
замін блочних симетричних шифрів

Виконав: студент 5 курсу, групи

БІКСм-12-1

напряму підготовки (спеціальності)

8.17010101, Безпека інформаційних та

комунікаційних систем

(шифр і назва напряму підготовки, спеціальності)

Фролов В.В.

(прізвище та ініціали)

Керівник

Кузнецов О.О.

(прізвище та ініціали)

Рецензент

Кошман С.О.

(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

Напрямок 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

“ ” 2013 року

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

Фролову Владиславу Володимировичу

(прізвище, ім'я, по батькові)

1. Тема магістерської атестаційної роботи: «Дослідження методів формування нелінійних вузлів заміन блочних симетричних шифрів»

керівник магістерської атестаційної роботи:

Кузнецов Олександр Олександрович, д.т.н., проф.

(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

“4” червень 2013 року

3. Вихідні дані до проекту (роботи): матеріали з опису та аналізу методів формування нелінійних вузлів замін.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

Вступ.

1 Критерії та показники стійкості блочних симетричних шифрів

2 Аналіз методів синтезу регулярних нелінійних вузлів замін

3 Дослідження методу імітації відпалу

4 Опис програми

5 Охорона праці та безпека в надзвичайних ситуаціях.

Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
презентаційні матеріали у вигляді слайдів.

6. Консультанти розділів магістерської атестаційної роботи.

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1, 2, 3, 4	Кузнецов О.О., 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	Вивчення та класифікація методів формування нелінійних вузлів замін	01.04 – 20.04	Виконано
3	Програмна реалізація роботи з нелінійними вузлами замін та їх формування методом імітації відпалу	21.04 – 05.05	Виконано
4	Виконання завдання з розділу «Охорона праці та безпека в надзвичайних ситуаціях»	06.05 – 10.05	Виконано
5	Проведення порівняльного аналізу основних методів формування нелінійних вузлів замін	11.05 – 15.05	Виконано
6	Програмне моделювання та дослідження властивостей сформованих вузлів замін	16.05 – 20.05	Виконано
7	Оформлення пояснювальної записки	21.05 – 26.05	Виконано

	Студент	_____	Фролов В.В.
		(підпис)	(прізвище та ініціали)
Керівник магістерської атестаційної роботи		_____	Кузнецов О.О.
		(підпис)	(прізвище та ініціали)