МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ І ІНФОРМАТИКИ

З А Г А Л Ь Н І В К А З І В К И

до виконання курсового проекту з дисципліни

«**Методи та засоби криптографічного захисту інформації**»

Д.т.н., проф. каф. ПМІ
Башков Є.О.

Покровськ – 2021

ВСТУП

Курсовий проект виконується на підставі навчального плану підготовки студентів за освітньо-кваліфікаційним рівнем «бакалавр» спеціальності 125 Кібербезпека та «Технічного завдання до курсового проекту» за дисципліною «Методи та засоби криптографічного захисту інформації».

Розробка проекту орієнтована на закріплення теоретичного матеріалу та придбання практичних навичок в використанні сучасних методів та алгоритмів криптографічного захисту інформації. Метою курсового проекту є:

- Подальше засвоєння особливостей криптографічних методів захисту інформації і зміст базових понять криптографії.
- Закріплення отриманих знань з математичних основ криптографічних методів захисту інформації;
- Закріплення уявлень про основні алгоритмічних проблеми криптографії і способах їх вирішення.
- Подальше засвоєння знань щодо спеціальних математичних структур, що застосовуються в криптографії
- Практичне застосування сучасних стандартних методів шифрування для побудови програмних засобів захисту інформації;

Процес виконання курсової роботи має підготувати студентів до подальших етапів навчальної (кваліфікаційна робота) та практичної діяльності.

1 ТЕМАТИКА КУРСОВОГО ПРОЕКТА

Загальне завдання на курсовий проект передбачає створення програмного додатку за двома загальними напрямками:

- розробку і дослідження основних і допоміжних алгоритмів криптографії, розробку засобів і протоколів захищеної передачі інформації по мережі, розробка засобів приховування інформації і т.д.,
- розробку інформаційних систем з підсистемами захисту інформації, аналіз прикладних рішень на їх стійкість до атак.

Також курсова робота включає оформлення пояснювальній записки, в

якій детально викладені цілі і завдання роботи, об'єкт дослідження, а також хід виконання роботи і докладний опис отриманого результату.

Мова програмування обирається студентом. Рекомендовано застосовувати мову Python. Можливі варіанти індивідуального завдання наведені в додатку.

2 ЗМІСТ ТА ЕТАПИ РОЗРОБКИ

При виконанні курсового проекту для кожного класу задач студент повинен:

- Надати математичний опис задачі та математичні співвідношення відповідного методу (алгоритму, протоколу, засобу) її вирішення.
- Описати відомі та прийнятий метод (алгоритм, протокол, засіб) вирішення задачі.
- Визначити тестові завдання для подальшої перевірки розробленого методу (алгоритму, протоколу, засобу).
- Розробити програмну реалізацію запропонованого методу (алгоритму, протоколу, засобу).
- Виконати тестування розробленої програмної реалізації за допомогою тестових завдань. Надати висновки щодо працездатності розробленої програмної реалізації та характеристик методу (алгоритму, протоколу, засобу).

Графік виконання курсового проекту наведено в табл. 1.

Таблиця 1 - Графік виконання курсового проекту

№	Найменування етапу	Строк виконання	
		тиждень	дата
1	Видача завдання на курсовий проект. З'ясування завдання. Опанування математичними співвідношеннями	1-2	
2	Визначення методу (алгоритму, протоколу, засобу) вирішення задачі проекту.	3-6	

3	Розробка тестових завдань	5-6	
4	Розробка програмної реалізації	6-9	
5	Тестування програмної реалізації	6-9	
6	Формулювання висновків	10-12	
7	Оформлення пояснювальної записки	13-14	
8	Захист курсового проекту	15-16	

Курсовий проект виконується з використанням довільної мови програмування. Рекомендовано використовувати мову Python в середовищі Anaconda (Spyder) або в MS Visual Studio в OS Microsoft Windows 10.

3 ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Загальні вимоги

Загальними вимогами текстової частини пояснювальної записки є:

- чіткість і логічна послідовність викладу матеріалу;

- переконливість аргументації;

- стислість і точність формулювань, що виключають можливість суб'єктивного й неоднозначного тлумачення;

- конкретність викладу результатів виконання проведеної роботи;

- доказовість і обґрунтованість рекомендацій і пропозицій;

- єдність термінів у межах роботи і їхня відповідність установленим стандартам, а при відсутності останніх - загальноприйнятим у науково-технічній літературі.

Не допускається використання в тексті «місцевих термінів», необхідно користуватися загальноприйнятими.

При викладі не допускається переписування загальних положень, а так само визначень із підручників, навчальних статей, посібників і інших джерел. При необхідності використання в текстовому документі матеріалів з літературних джерел, необхідно робити на них посилання по тексту.

Структурні частини текстового документа починають із нового аркуша, їх не нумерують. Заголовки структурних одиниць записуються по центру й прописними буквами; підрозділи з нового рядка й тільки перша буква прописна.

Сторінки нумеруються арабськими цифрами. Нумерація сторінок наскрізна по всьому текстовому документу й проставляється в правому верхньому куті сторінки. Титульний аркуш, список виконавців, завдання не нумеруються, але входять у загальне число сторінок.

При написанні пояснювальної записки використовується шрифт Times New Roman, розмір 14, накреслення Звичайний. Забороняється використовувати накреслення Курсив, Підкреслення й Напівжирний.

Обов'язкові складові пояснювальної записки:

- титульний аркуш;
- анотація українською та англійською мовами;
- завдання на курсовий проект;
- зміст;
- вступ;
- основна частина (1 – 3 розділи);
- висновки;
- перелік посилань;
- додатки із текстом розроблених модулів;
- додатки із технічною документацією на розроблені модулі;

4 ПОРЯДОК КОНТРОЛЮ Й ПРИЙОМУ

Курсовий проект виконується 16 тижнів. Пояснювальна записка до курсового проекту надається на перевірку викладачам не менш чим **за 3 робочі дні** до дати захисту.

Захист відбувається в присутності комісії в складі 2-3 осіб і включає:

а) доповідь, що відбиває всі етапи проектування курсового проекту;

б) презентацію роботи модулю;

в) відповіді на запитання комісії.

Шкала оцінювання виконання курсового проекту

Теоретичне обґрунтування	Виконання програмного опису	Оформлення пояснювальної записки	Виступ з презентацією	Максимальна сума балів
30	**30**	**20**	**20**	**100**

5 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Вильямс, 2016.
2. Задірака В.К., Олексюк О.С.,.Недашковський М.О. Методи захисту фінансової інформації. Навчальний посібник. К.: Вища школа, 2000. – 460 с
3. Молдовян Н. А. Молдовян Н.А. Теоретический минимум и алгоритмы цифровой подписи. - СПб.: БХВ-Петербург, 2010. - 293 с. - (Учебное пособие) http://znanium.com/bookread.php?book=351283.
4. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. Криптология. — Минск: БГУ, 2013.
5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. — Москва: Гелиос АРВ, 2001.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328с.

7. Домарев В.В. Защита информации и безопасность компьютерных систем. - К.: Издательство «Диасофт», 1999. – 480с.
8. Рябко, Б. Я. Основы современной криптографии и стеганографии [Электронный ресурс]. - М. : Горячая линия-Телеком, 2010. - 232 с.
9. Герман, О. Н. Теоретико-числовые методы в криптографии: учебник для студентов учреждений высшего профессионального образования, обучающихся по направлениям подготовки "Информационная безопасность" и "Математика" / О. Н. Герман, Ю. В. Нестеренко. - Москва: Академия, 2012. - 272 с.
10. Романьков, В. А. Введение в криптографию: курс лекций / В. А. Романьков. - 2-е изд., испр. и доп. - М.: Форум, 2012. - 240 с.
11. Гашков, С. Б. Криптографические методы защиты информации : учеб. Пособие для студ. вузов. - М.: Академия, 2010.
12. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых.-К.: Изд. «Политехника», 2004. – 224с.