МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЗ „ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА"

Кафедра алгебри та системного аналізу

РОБОЧА ПРОГРАМА

навчальної дисципліни **Криптографічний захист цифрової інформації**
(назва дисципліни)
для третього освітньо-наукового рівня доктор філософії (PhD)

напряму / спеціальності 111 Математика

ЗАТВЕРДЖЕНО

на засіданні кафедри
протокол № 4 від 26.11.2019 р.

ВІДДІЛ АСПІРАНТУРИ

Завідувач кафедри проф. Жучок А.В. _____ (підпис)

Перезатверджено: протокол №_____ від _____

Перезатверджено: протокол №_____ від _____

Перезатверджено: протокол №_____ від _____

Старобільськ – 2019

1. **Назва дисципліни.**

КРИПТОГРАФІЧНИЙ ЗАХИСТ ЦИФРОВОЇ ІНФОРМАЦІЇ

2. **Код дисципліни.**

ВПП2

3. **Тип дисципліни.**

Вибіркова

4. **Рік (роки) навчання.**

1-й

5. **Семестр / семестри.**

2

6. **Кількість кредитів ECTS.**

3,0

7. **Відомості про викладача (викладачів)**.

Тоічкіна Олена Олександрівна – старший викладач кафедри алгебри та системного аналізу, кандидат фізико-математичних наук, e-mail: toichkina.e@gmail.com.

8. **Мета вивчення дисципліни (в термінах результату навчання й компетенції).**

Мета – формування в аспірантів знань про основні принципи криптографічних методів і алгоритмів захисту цифрової інформації, а також практичних навичок безпечної роботи в інформаційних системах.

9. **Передумови (актуальні знання, необхідні для опанування дисципліни).**

Вивчення дисципліни “Криптографічний захист цифрової інформації” передбачає наявність систематичних та ґрунтовних знань з таких курсів, як „Лінійна алгебра та аналітична геометрія”, “Дискретна математика”, “Загальна алгебра”, “Алгоритми та структури даних”, “Математична логіка та теорія алгоритмів”.

10. **Зміст дисципліни.**

№	Змістовні модулі та їхня структура	денна форма навчання					заочна форма навчання				
		загальна кількість	Лекції	практичні заняття	лабораторні роботи	самостійна робота	загальна кількість	Лекції	практичні заняття	лабораторні роботи	самостійна робота
Перший модуль											
Тема 1. Криптографія як наукова дисципліна											
1.1.	Основні поняття та предмет криптографії.	3	1			2					
1.2.	Задачі криптографії.	2				2					
1.3.	Математичні основи криптографії.	9	1			8					
Тема 2. Криптосистеми з закритим ключем											
2.1.	Загальна схема симетричного шифрування.	4		2		2					
2.2.	Методи шифрування з закритим ключем.	8	2	2		4					
Тема 3. Криптографічні алгоритми з відкритим ключем											

3.1.	Основні поняття, властивості та класифікації асиметричних методів шифрування.	4				4					
3.2.	Методи побудови асиметричних криптосистем.	6	2	2		2					
Другий модуль											
Тема 4. Електронний цифровий підпис											
4.1.	Поняття електронного цифрового підпису.	5				5					
4.2.	Алгоритми створення цифрового підпису та його перевірки на основі криптосистем з відкритими ключами.	9	2	2		5					
4.3.	Детерміновані цифрові підписи: криптосистема RSA, генерація й перевірка підпису, проблема безпеки.	12	2	2		8					
4.4.	Ймовірнісні цифрові підписи: криптосистема Ель-Гамаля, генерація й перевірка підпису, проблема створення прихованого каналу передачі повідомлень.	12	2	2		8					
Тема 5. Криптографія на еліптичних кривих											
5.1.	Рівняння еліптичної кривої. Використання еліптичних кривих у криптографії.	9	2	2		5					
5.2.	Цифровий підпис на еліптичних кривих.	7	2			5					
ЗАГАЛЬНА КІЛЬКІСТЬ ГОДИН		**90**	**16**	**14**		**60**					

11. Список рекомендованої навчальної літератури.

Основна навчальна література

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах. – К.: КМ Академія, 2006. – 244 с.
2. Венбо Мао. Современная криптография. Теория и практика. М: Вильямс, 2005. – 768 с.
3. Бернет С., Пэйн С., Криптография. Официальное руководство RSA Security. Изд. 2-е, стереотипное. – М.: ООО «Бином-Пресс», 2007. – 384 с.: ил.
4. Аграновский А.В., Хади Р.А. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2002. – 256 с.
5. Адаменко М.В. Основы классической криптологии: секреты шифров и кодов. – М.: ДМК Пресс, 2012. – 256 с.
6. Бабаш А. В. Криптография. – М.: СОЛОН-Пресс, 2007. – 511 с.
7. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии: Учебное пособие. М.: Горячая Линия - Телеком, 2002. – 175 с.
8. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. М.: Издательство: АНО НПО "Профессионал", 2005. – 480 с.
9. Столлингс В. Криптография и защита сетей: принципы и практики, 2-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2007. – 672 с.
10. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнійчук, 2011. – 152 с.

Додаткова навчальна література

1. Фергюссон Н. Практическая криптография / Н. Фергюссон, Б. Шнайер. – М.: Вильямс, 2005. – 424 с.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2006. – 336 с.

3. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук // Видання друге, виправлене, – Тернопіль: ТзОВ “Терно-граф”, 2010. – 536 с.
4. Ян С. Криптоанализ RSA / С. Ян. — Ижевск: РХД. 2011. — 312 с.
5. Srivastava A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem / A. Srivastava, A. Mathur // International Journal of Scientific and Research Publications. – 2013. – Vol. 3 (6). – P. 1-4.
6. Hayder R.H. H-Rabim Cryptosystem / R.H. Hayder // Journal of Mathematics and Statistics. - 2014. – Vol. 10 (3). – P. 304-308.
7. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. – М.: ТВП. – 2001. – 254с.

12. Технології викладання та атестації.

Діяльність студента:

- опанування теоретичного матеріалу;
- самопідготовка (повторення матеріалу підручників та навчальних посібників, підготовка до практичних занять, поточного та підсумкового контролю);
- поточний контроль теоретичних знань під час проведення практичних робіт;
- написання контрольних модульних робіт.

Поточний контроль:

- виконання практичних завдань;
- дві письмові модульні контрольні роботи.

Форма семестрового контролю:

іспит.

13. Критерії оцінювання (у %).

Семестрову рейтингову оцінку розраховують, виходячи з критеріїв:

- письмові модульні контрольні роботи – 65%;
- результати виконання практичних робіт – 35%.

14. Мови викладання.

Українська.