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

Кафедра алгебри та системного аналізу

СИЛАБУС

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.

Завідувач кафедри проф. Жунок 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

Кількість кредитів ECTS.

3,0

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

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

7. **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.

8. **Компетенції здобувача, які формуються внаслідок вивчення дисципліни**

В результаті освоєння освітньо-наукової програми освітнього рівня доктора філософії у здобувача мають бути сформовані такі компетентності:

- інтегральна компетентність (ІК), здатність розв'язувати комплексні проблеми в галузі професійної та/або дослідницько-інноваційної діяльності;
- загальні компетентності (ЗК), які не залежать від галузі та є обов'язковими для здобувачів ступеню доктора філософії;
- фахові компетентності (ФК), які розкривають вміння та навички здобувачів ступеню доктора філософії.

Таблиця 1. Компетентності та програмні результати навчання згідно з Освітньо-науковою програмою доктора філософії 111 Математика.

ВПП2	Криптографічний захист цифрової інформації	3,0	ІК, ЗК4, ЗК6, ЗК7, ЗК8, ЗК11, ЗК15, ЗК18, ЗК19, ЗК20, ЗК21, ЗК22, ЗК23, ЗК32, ЗК33, ФК3, ФК4, ФК10, ФК11, ФК18, ФК22, ФК23, ФК24, ФК25, ФК26, ФК27, ФК28, ФК29, ФК30	ПРН-З-2, ПРН-З-13, ПРН-З-14, ПРН-З-21, ПРН-З-22, ПРН-З-28, ПРН-З-29, ПРН-З-30, ПРН-У-10, ПРН-У-14, ПРН-У-16, ПРН-У-24, ПРН-У-25, ПРН-У-32, ПРН-У-33

Знання:

- знання основних понять, законів і методів криптографічного захисту інформації;
- знання основних етапів історичного розвитку криптографії;
- знання принципів побудови сучасних криптосистем;
- знання математичних основ криптографії;

- знання основних вимог до шифрів та їх характеристики;
- знання основних способів шифрування даних;
- знання класифікації шифрів;
- знання принципу побудови криптографічних алгоритмів та криптографічних стандартів, їх використання в задачах захисту інформації;
- знання основних положень нормативно-правового регулювання у галузі криптографічного захисту інформації;
- знання основних напрямів розвитку сучасних систем криптографічного захисту інформації;
- знання основних підходів до реалізації криптографічних засобів захисту інформації;
- знання змісту стандартних і складних задач асиметричної криптографії з використанням ІКТ.

Уміння:

- вільне володіння фундаментальними поняттями криптографії, основними математичними методами криптографічного захисту інформації, засобами побудови типових криптографічних алгоритмів;
- уміння оцінювати складність криптографічної системи;
- уміння створювати, оцінювати та застосовувати сучасні криптографічні алгоритми розподілу ключів і цифрового підпису;
- уміння створювати нові криптографічні алгоритми захисту інформації;
- уміння оцінювати і запобігати загрозам безпеки інформаційних ресурсів методами криптографії;
- уміння діагностувати, аналізувати і консультувати в галузі ІТ рішень;
- уміння розробляти інформаційні системи та застосовувати до розробки, аналізу і верифікації алгоритмів і програмних систем і комплексів;
- уміння обґрунтовувати та висувати пропозиції щодо стандартних криптографічних систем захисту ресурсів у комп'ютерних системах та комп'ютерних мережах;
- уміння використовувати програмні засоби, які реалізують основні криптографічні функції;
- уміння програмно реалізовувати криптографічні алгоритми розв'язання типових задач захисту інформації;
- уміння проектувати криптографічні системи захисту різного рівня;
- уміння використовувати методи та засоби криптографічного захисту даних;
- уміння обирати необхідні криптографічні методи та алгоритми для розв'язання практичних задач інформаційної безпеки.

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	3	1			2					

	криптографії.										
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;
- 2 письмові модульні контрольні роботи.

Форма семестрового контролю:

2 семестр – 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.

15. Навчальний контент до проведення практичних робіт

Теми практичних робіт

Перший модуль

1. Загальна схема системи захисту інформації. Побудова функцій шифрування.
2. Симетричні системи захисту інформації.
3. Асиметричні системи захисту інформації.

Другий модуль

1. Електронний цифровий підпис.
2. Система захисту RSA.
3. Реалізація цифрового підпису на основі криптосистеми Ель-Гамаля.
4. Шифрування та розшифрування з використанням еліптичних кривих.

16. Навчальний контент до організації самостійної роботи

Теми для самостійного вивчення

Тема 1. Криптографія як наукова дисципліна.

1. Однобічні функції.
2. Задачі криптографії.
3. Проблеми безпеки інформації: конфіденційність, цілісність, аутентифікація, цифровий підпис.
4. Управління секретними ключами: попереднє розподілення ключів, пересилання ключів, відкритий розподіл ключів.
5. Схема розділення секрету.
6. Формальні моделі простих шифрів.
7. Формальні моделі шифрів.
8. Математична модель відкритого тексту.
9. Критерії розпізнавання відкритого тексту.
10. Класифікація шифрів за різними ознаками
11. Математична модель шифру заміни.
12. Класифікація шифрів заміни.
13. Поточні шифри.

Тема 2. Криптосистеми з закритим ключем.

1. Метод простої підстановки (заміни): шифр Полібія, шифр Віженера.
2. Метод перестановки.
3. Метод блочних шифрів.
4. Метод гамірування.
5. Метод шифрування на основі теореми Ейлера-Ферма.
6. Композиція шифрів.
7. Симетричні системи захисту інформації: криптосистема Хілла, шифрування за допомогою афінних перетворень, шифр Плейфейра, парний шифр.
8. Стандарт криптосистеми DES.
9. Стандарт криптосистеми ГОСТ.

Тема 3. Криптографічні алгоритми з відкритим ключем.

1. Числовий варіант системи захисту RSA.
2. Системи захисту інформації Діффі-Хеллмана.
3. Системи захисту інформації на основі заданого рюкзака.
4. Система захисту інформації на основі кода Варшамова.
5. Узагальнена рюкзачна криптосистема з відкритим ключем.
6. Системи захисту інформації на основі розв’язань багатостепеневих систем діофантових рівнянь.

Тема 4. Електронний цифровий підпис.

1. Цифровий підпис Фіата-Шаміра.
2. Підписи ElGamal.
3. DSA.
4. Алгоритм цифрового підпису ГОСТ 34.10-94.
5. Дерева цифрових підписів.
6. Підпис документа за допомогою криптографії з відкритим ключем.

Тема 5. Криптографія на еліптичних кривих.

1. Побудова криптосистем на еліптичних кривих.
2. Дискретний логарифм на *E*.
3. Аналог ключового обміну Діффі-Хеллмана.
4. Аналог системи Мессі-Омури.
5. Застосування еліптичних кривих.
6. Безпека криптографії з використанням еліптичних кривих.

17. Проведення поточного і підсумкового контролю

Завдання до контрольної модульної роботи №1

Варіант 1

1. Нехай x_1, x_2, x_3 – корні многочлена $\varphi(x) = x^3 + x - 7.$ Зашифрувати повідомлення

T = НЕ_ПОМИЛИСЬ

за допомогою функції $f(x) = 2x^7 + 7x^5 - 14x^4 - 4x^3 - 35x^2 - x + 10$ таким чином: $e = f(x_k) + s,$ де s – числовий еквівалент поточної літери, а x_k – довільний корінь $\varphi(x).$

2. Нехай криптограма деякого відкритого тексту має вигляд: ІЩЧЯРШГИЦЮЮ:

$$(25+17) \bmod 33 = 09 \Rightarrow y_1 = I;$$
$$(09+17) \bmod 33 = 26 \Rightarrow y_2 = Щ;$$
$$(21+03) \bmod 33 = 24 \Rightarrow y_3 = Ч;$$
$$(17+15) \bmod 33 = 32 \Rightarrow y_4 = Я;$$
$$(33+17) \bmod 33 = 17 \Rightarrow y_5 = Р;$$
$$(08+17) \bmod 33 = 25 \Rightarrow y_6 = Ш;$$
$$(01+03) \bmod 33 = 04 \Rightarrow y_7 = Г;$$
$$(13+15) \bmod 33 = 28 \Rightarrow y_8 = И;$$
$$(06+17) \bmod 33 = 23 \Rightarrow y_9 = Ц;$$
$$(14+17) \bmod 33 = 31 \Rightarrow y_10 = Ю;$$
$$(28+03) \bmod 33 = 31 \Rightarrow y_11 = Ю.$$

Провести криптоаналіз і розкрити цей шифр.

3. При зашифруванні блоку T системи DES його біти піддаються початковій перестановці IP:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Визначити кінцеву перестановку $IP^{-1}.$

4. Довести, що ін'єктивний рюкзачний вектор $A = (1, p, p^2, ..., p^{n-1})$ є водночас і щільним.

5. Провести порівняльний аналіз систем ГОСТ 28147-89 і DES.

Варіант 2

1. Зашифрувати повідомлення Т=ЗУСТРІЧ_СКАСОВУЄТЬСЯ_ЯВКУ_РОЗКРИТО за допомогою ключа з таблиці:

t	1	2	3	…	n
e	[0, 1)	[1, 2)	[2, 3)	…	[n–1, n)

2. Довести, що якщо $P \equiv 1 (\bmod 4)$, то P можна представити у вигляді суми двох натуральних чисел єдиним способом. З урахуванням доведеного зашифрувати текст:

T=ХОТНАR_КНОТАL

3. Визначити прості ключі шифртекста: E=ТЕАГАШ_НАВАРАК_ТЕАЛ_АКАБОС та розшифрувати його.

4. Довести, що узагальнений рюкзачний вектор $\tilde{A}_p = (a_1, a_2, ..., a_n)$ розмірності $n,\ n \geq 3$ є щільним та ін'єктивним, якщо $a_1 = c,\ a_J = p^{J-2} * ((p-1)c + 1),\ J = 2..n,$ де с – деяка ціла додатна константа.

5. Провести порівняльний аналіз систем ГОСТ 28147-89 і DES.

Завдання до контрольної модульної роботи №2

Варіант 1

1. Вихідний текст SAUNA зашифровано як TAKE BACK VAT OR BONDS. Опишіть криптосистему, яку було використано.

2. У криптосистемі з блочним шифром Хілла і з матрицею $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ зашифруйте текст PAYMOREMONEY.

3. Побудуйте криптосистему Ель-Гамаля для p=19 і підпишіть повідомлення *M* = ВЕРНИСЬ_В_АРЦАХ.

4. Розробити алгоритм реалізації цифрового підпису для відомої вам криптосистеми.

Варіант 2

1. Вихідний текст SAUNAANDLIFE зашифровано як RMEMHCZZTCEZTZKKDA. Опишіть криптосистему, яку було використано.

2. У криптосистемі з блочним шифром Хілла і з матрицею $\begin{pmatrix} 11 & 2 & 19 \\ 5 & 23 & 25 \\ 20 & 7 & 1 \end{pmatrix}$ зашифруйте текст STOPPAYMENTX.

3. Побудуйте криптосистему Ель-Гамаля для p=19 і підпишіть повідомлення *M* = ВЕРНИСЬ_В_АРЦАХ.

4. Розробити алгоритм реалізації цифрового підпису для відомої вам криптосистеми.

Запитання до підсумкового контролю

1. Мета і завдання дисципліни.
2. Основні поняття та визначення.
3. Роль криптографії у захисті даних.
4. Розробка та аналіз простих криптографічних алгоритмів на основі методів перестановок та підстановок.
5. Генерація псевдовипадкових послідовностей чисел в системах захисту інформації.
6. Оцінка статистичних характеристик датчика псевдовипадкових чисел із заданим законом розподілу.
7. Розробка і реалізація варіанту симетричного криптографічного алгоритму з DES – подібною структурою.
8. Оцінка швидкості роботи криптоалгоритму.
9. Розробка алгоритму та програмна реалізація атаки на симетричну криптографічну систему.
10. Програмна реалізація алгоритму RSA.
11. Розробка і програмна реалізація протокола обміну симетричними ключами.
12. Розробка і програмна реалізація алгоритму обчислення цифрового дайджеста повідомлення.
13. Програмна реалізація алгоритмів цифрового підпису.
14. Потрійний DES. Сфери застосування різних режимів DES.
15. Схема режиму шифрування простої заміни ГОСТ 28147-89.
16. Реалізація алгоритму шифрування RSA.
17. Реалізація алгоритму шифрування Ель-Гамаля.
18. Алгоритм шифрування на основі задачі про укладку портфеля.
19. Реалізація алгоритму шифрування на основі еліптичних кривих.
20. Реалізація основних криптографічних протоколів.
21. Реалізація протоколів обміну ключами.
22. Реалізація протоколів аутентифікації.
23. Реалізація парольної ідентифікації/аутентифікації.

24. Реалізація протоколу ідентифікації/аутентифікації на основі шифрування з відкритим ключем.
25. Ідентифікація/аутентифікація з допомогою біометричних даних.
26. Реалізація електронного цифрового підпису.
27. Реалізація ЕЦП на базі алгоритму RSA.
28. Реалізація ЕЦП на базі алгоритму DSA.
29. Реалізація алгоритму цифрового підпису ГОСТ 34.10-94.
30. Реалізація алгоритму цифрового підпису ГОСТ 34.10-2001.