МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Кафедра захисту інформації

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Основи криптографії та стеганографії

Освітня програма: Безпека інформаційних і комунікаційних систем

Спеціальність: 125 Кібербезпека

Галузь знань: 12 Інформаційні технології

Ступінь вищої освіти: Перший (бакалаврський) рівень

Затверджено на засіданні кафедри
захисту інформації
Протокол №____ від _____ р.

м. Запоріжжя 2020

1. Загальна інформація	
Назва дисципліни	*ППН 07. Основи криптографії та стеганографії, обов'язкова.*
Рівень вищої освіти	*Перший (бакалаврський) рівень*
Викладач	*Козіна Галина Леонідівна, к.ф.-м.н., доцент.*
Контактна інформація викладача	*Телефон кафедри 7698491, викладача 7698597, kozina@zp.edu.ua*
Час і місце проведення навчальної дисципліни	*Згідно розкладу занять викладачів кафедри.* https://zp.edu.ua/kafedra-zahistu-informaciyi
Обсяг дисципліни	*9 кредитів ЄКТС, 270 годин.* *Розподіл годин:* *- 7,5 кредитів ЄКТС, 225 годин теоретичні та практичні заняття, лекції 60 годин, лабораторні 30 годин, самостійна робота 135 годи.* *– 1,5 кредитів ЄКТС, 45 годин, курсова робота.* *Семестр вивчення навчальної дисципліни: 6 і 7 семестри.* *Вид контролю: залік в кінці 6 семестру і іспит в кінці 7 семестру, захист курсової роботи в кінці 7 семестру.*
Консультації	*Згідно з графіком консультацій.* https://zp.edu.ua/kafedra-zahistu-informaciyi

2. Пререквізити і постреквізити навчальної дисципліни

Пререквізити: Вища математика (теми: лінійна алгебра, математичний аналіз, аналітична геометрія), Теорія інформації і кодування (теми: поняття інформації, повідомлення, сигналу, коду).

Компетентності:

КЗ 1. Здатність застосовувати знання в практичних ситуаціях.

КЗ 8. Здатність використовувати знання базових розділів фізики і математики в обсязі, необхідному для засвоєння фахових дисциплін.

Постреквізити: Протоколи цифрового підпису, Безпека інформаційно-комунікаційних систем.

3. Характеристика навчальної дисципліни

Дисципліна «Основи криптографії та стеганографії" є базовою у підготовці фахівця з інформаційної безпеки.

Перелік загальних и фахових компетентностей, яких набуває студент при вивченні:

КЗ 4. Вміти виявляти, ставити та вирішувати проблеми за професійним спрямуванням, здійснювати професійну діяльність на основі техніко-економічного аналізу.

КЗ 8. Здатність використовувати знання базових розділів фізики і математики в обсязі, необхідному для засвоєння фахових дисциплін.

КФ 1. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах

КФ 3. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки.

КФ 6. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 11. Здатність застосовувати методи та засоби криптографічного, стеганографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

Програмні результати навчання:

ПРН 8. Використовувати знання про фізичні явища та володіти математичним апаратом для моделювання об'єктів інформаційної діяльності

ПРН 9. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки

ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.

ПРН 31 Вирішувати задачі захисту інформації, що обробляється в інформаційно-

телекомунікаційних системах з використанням сучасних методів та засобів криптографічного та стеганографічного захисту інформації.

4. Мета вивчення навчальної дисципліни

Формування у студентів здатності застосовувати стандартні криптографічні алгоритми та протоколи для захисту інформації.

5. Завдання вивчення дисципліни

Основне завдання навчальної дисципліни – формування у студентів системних знань і компетенностей з теоретичних та практичних знань математичних основ криптографії, криптографічних перетворень інформації, криптоалгоритмів та криптопротоколів, оцінки їх криптостійкості та використання в інформаційних і телекомунікаційних системах.

6. Зміст навчальної дисципліни

Перший семестр. Модуль 1.

Змістовий модуль 1.

Тема 1. Поняття теорії чисел. Перевірка чисел на простоту. Прості шифри.

Тема 2. Лінійні рекурентні послідовності. Факторизація чисел.

Змістовий модуль 2.

Тема 3. Асиметричний алгоритм шифрування RSA.

Тема 4. Схема Діффі-Хеллмана в мультиплікативній групі.

Тема 5. Китайський стандарт шифрування для захисту бездротових мереж SM4.

Другий семестр. Модуль 2.

Змістовий модуль 1.

Тема 6. Еліптичні криві над простим полем.

Тема 7. Схема Діффі-Хеллмана на еліптичних кривих.

Тема 8. Стандарт цифрового підпису ECDSA над простим полем.

Змістовий модуль 2.

Тема 9. Еліптичні криві над розширеним полем. Український стандарт цифрового підпису ДСТУ 4145-2002.

Тема 10. Американський стандарт шифрування FIPS 197.

Тема 11. Український стандарт шифрування ДСТУ 7624:2014.

Тема 12. Основні поняття стеганографії.

7. План вивчення навчальної дисципліни

№ тижня	Назва теми Форми організації навчання		Кількість годин
	Перший семестр		
1	*Поняття теорії чисел.*	лк	2
	Лабораторна робота №1. Поняття теорії чисел.	лб	2
2	*Перевірка чисел на простоту.*	лк	2
3	*Прості шифри. Частотний криптоаналіз.*	лк	2
	Лабораторна робота №2. Прості шифри.	лб	2
4	*Розв'язання порівнянь першого ступеня.*	лк	2
5	*Рекурентні співвідношення*	лк	2
	Лабораторна робота №3. Лінійні рекурентні послідовності.	лб	2
6	*Піднесення до ступеня за модулем.*	лк	2
7	*Розкладання чисел на множники.*	лк	2
	Лабораторна робота №4. Факторизація чисел.	лб	2
	Рубіжний контроль.		
8	*Асиметрична криптографія.*	лк	2
9	*Асиметричний алгоритм шифрування RSA.*	лк	2
	Лабораторна робота №5. Асиметричний алгоритм шифрування RSA.	лб	2
10	*Елементи теорії груп.*	лк	2

11	*Схема Діффі-Хеллмана в мультиплікативній групі.*	лк	2
	Лабораторна робота №6. Схема Діффі-Хеллмана в мультиплікативній групі.	лб	2
12	*Функції хешування.*	лк	2
13	*Задача дискретного логарифмування.*	лк	2
	Лабораторна робота №7. Дискретний логарифм.	лб	2
14	*Схема цифрового підпису на базі RSA.*	лк	2
15	*Китайський стандарт шифрування для захисту бездротових мереж SM4.*	лк	2
	Лабораторна робота №8. Основні криптоперетворення в китайському стандарті шифрування SM4.	лб	2
Рубіжний контроль. Підсумковий семестровий контроль - залік.			
Другий семестр			
1	*Прості поля.*	лк	2
2	*Еліптичні криві над простим полем.*	лк	2
	Лабораторна робота №9. Еліптичні криві над простим полем.	лб	2
3	*Розв'язання квадратного рівняння в простому полі.*	лк	2
4	*Дискретний логарифм в групі точок еліптичної кривої.*	лк	2
	Лабораторна робота №10. Дискретний логарифм в групі точок еліптичної кривої.	лб	2
4	*Протоколи передачі секретного ключа.*	лк	2
6	*Схема Діффі-Хеллмана на еліптичних кривих.*	лк	2
	Лабораторна робота №11. Схема Діффі-Хеллмана на еліптичних кривих.	лб	2
7	*Сучасні стандарти цифрового підпису.*	лк	2
8	*Стандарт цифрового підпису ECDSA над простим полем.*	лк	2
	Лабораторна робота №12. Стандарт цифрового підпису ECDSA над простим полем.	лб	2
Рубіжний контроль.			
9	*Еліптичні криві над розширеним полем.*	лк	2
10	*Український стандарт цифрового підпису ДСТУ 4145-2002.*	лк	2
	Лабораторна робота №13. Український стандарт цифрового підпису ДСТУ 4145-2002.	лб	2
11	*Сучасні стандарти шифрування.*	лк	2
12	*Американський стандарт шифрування FIPS 197.*	лк	2
	Лабораторна робота №14. Основні криптоперетворення в американському стандарті шифрування FIPS 197 (алгоритм RIJNDAEL)	лб	2
13	*Процедура розширення ключа в алгоритмі RIJNDAEL.*	лк	2
14	*Український стандарт шифрування ДСТУ 7624:2014.*	лк	2
	Лабораторна робота №15. Основні	лб	2

	криптоперетворення в українському стандарті шифрування ДСТУ 7624:2014.		
15	*Основні поняття стеганографії.*	лк	2
Рубіжний контроль. Підсумковий семестровий контроль - іспит.			

8. Самостійна робота

Самостійна робота включає в себе: вивчення теоретичного матеріалу, підготовку до лабораторних робіт, виконання курсової роботи, підготовку до рубіжного та підсумкового контролю.

8.1 Курсова робота

Мета курсової роботи - закріплення навичок в аналізі та розробці криптографічних алгоритмів захисту інформації, набутих під час виконання циклу лабораторних робіт.

Досвід, отриманий в ході виконання курсової роботи, може бути використаний для роботи над дипломним проектом (роботою) і в майбутній інженерній діяльності.

В процесі цієї роботи студент повинен навчитися вибрати і науково обґрунтувати прийняті проектні рішення; застосовувати сучасні, найбільш ефективні методи розрахунку і засоби обчислювальної техніки; користуватися спеціальною науковою і довідковою літературою, діючими стандартами та патентними матеріалами.

Завдання на курсову роботу розроблюється керівником курсової роботи і відображає сучасні тенденції в криптографії та стеганографії. Курсова робота оформлюється студентом згідно стандарту ДСТУ 3008-95.

Склад, обсяг і терміни виконання курсової роботи дисципліни наведені у таблиці.

№ тижня	Назва теми	Кількість годин
1-5	*Ознайомлення із завданням, підбір і аналіз літератури*	15
6-10	*Проведення необхідних обчислень*	15
11-15	*Оформлення і захист курсової роботи*	15
Усього годин		45

8.2 Самостійна робота з теорії та практиці дисципліни.

№ тижня	Назва теми	Кількість годин	Косультації, годин
	Перший семестр		
1-2	*Поняття теорії чисел.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
3-4	*Прості шифри. Частотний криптоаналіз.*	*4*	*0,5*
	Підготовка до лабораторних занять	*4*	*0,5*
5-6	*Рекурентні співвідношення.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
7	*Розкладання чисел на множники.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*10*	*1*
8-9	*Асиметричний алгоритм шифрування RSA.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
10--11	*Схема Діффі-Хеллмана в мультиплікативній групі.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
12-13	*Дискретний логарифм.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
14-15	*Китайський стандарт шифрування для захисту бездротових мереж SM4.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
Підготовка до рубіжного контролюю. Рубіжний контроль.		*6*	*1*
Підсумковий семестровий контроль - залік.		*10*	*1*

Другий семестр			
1-2	*Еліптичні криві над простим полем.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
3-4	*Дискретний логарифм в групі точок еліптичної кривої.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
5-6	*Схема Діффі-Хеллмана на еліптичних кривих.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
7	*Стандарт цифрового підпису ECDSA над простим полем.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*6*	*1*
8-9	*Український стандарт цифрового підпису ДСТУ 4145-2002.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
10-11	*Американський стандарт шифрування FIPS 197.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
12-13	*Український стандарт шифрування ДСТУ 7624:2014.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
14-15	*Основні поняття стеганографії.*	*4*	*0,5*
	Підготовка до лабораторних занять.	*4*	*0,5*
Підготовка до рубіжного контролю. Рубіжний контроль.		*6*	*1*
Підсумковий семестровий контроль - іспит.		*10*	*1*

9. Система та критерії оцінювання курсу

Поточний, рубіжний, семестровий контроль (з урахуванням відвідування занять, виконання лабораторних робіт, тестування при здачі модулів та заліку).

Форма проведення контролю: усна, письмова, комбінована, а також шляхом тестування з використанням програмно-технічних засобів.

9.1 Розподіл балів, які отримують студенти

Рубіжний контроль					
Змістовий модуль №1			*Змістовий модуль № 2*		
Тема 1-Тема 7	*Лабораторна робота №1-№4*	*Сума 1*	*Тема 8-Тема 15*	*Лабораторна робота №5-№8*	*Сума 2*
40	*60*	*100*	*40*	*60*	*100*

Підсумковий семестровий контроль					
Бали за змістові модулі	*Сума*	*Бали за семестровий контроль*	*Сума*	*Залік*	*Сума*
0.4 (Сума 1+ Сума 2)	*80*		*20*		*100*

9.2 Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	*Оцінка ECTS*	*Оцінка за національною шкалою*	
		для екзамену, курсового проекту (роботи), практики	*для заліку*
90 – 100	***A***	*відмінно*	*зараховано*
82-89	***B***	*добре*	
74-81	***C***		
64-73	***D***	*задовільно*	
60-63	***E***		
35-59	***FX***	*незадовільно з можливістю повторного складання*	*не зараховано з можливістю повторного складання*
0-34	***F***	*незадовільно з обов'язковим повторним вивченням дисципліни*	*не зараховано з обов'язковим повторним вивченням дисципліни*

10. Політика курсу

Викладач пояснює студентам систему організації навчального процесу та правил поведінки студентів на заняттях. Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Успішність засвоєння навчального матеріалу визначається числом балів, отриманих при контрольних заходах. Максимальне число балів за змістовий модуль дорівнює 100: 40 балів за результатами тестування з теоретичного матеріалу, 60 балів за

виконання 4 лабораторних робіт. Кожна лабораторна робота оцінюється 15 балами: 5 балів за відповіді на контрольні питання до роботи, 10 балів за виконання і захист роботи. Максимальне число балів підсумкового семестрового контролю дорівнює 100 і складаються: з суми балів змістових модулів, помноженої на коефіцієнт 0,4 - разом 80 балів, і додаткових 20 балів при опитуванні під час заліку. Студенти, які отримали при змістовому модульному контролі менше 60 балів до підсумкового семестрового контролю не допускаються.

Під час навчання студенти зобов'язані дотримуватися академічної доброчесності:

- самостійно виконувати навчальні завдання, завдання поточного та підсумкового контролю;
- дотримуватися норм законодавства про авторське право;
- приймати активну участь у навчальному процесі;
- не запізнюватися на заняття, не пропускати заняття без поважних причин;
- самостійно і своєчасно вивчити матеріал пропущеного заняття;
- давати достовірну інформацію про результати власної навчальної діяльності.
- бути терпимим і доброзичливим до однокурсників та викладачів.

Інформаційні ресурси:

https://zp.edu.ua
http://library.zp.edu.ua:8081/lib2web/DocSearchForm
http://e-library.zp.edu.ua
https://zp.edu.ua/kafedra-zahistu-informaciyi