ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

ЗАТВЕРДЖУЮ
Декан ФІТ
_____ Говорущенко Т.О.
«05» вересня 2024 р.

СИЛАБУС

Вибіркова дисципліна **Криптологія**

Загальна інформація

Позиція	Зміст інформації
Викладач	**Капустян Марія Вікторівна**
Профайл викладача	http://kiis.khmnu.edu.ua/personnel/kapustyan-mariya-viktorivna/
E-mail викладача	kapustianm@khnu.edu.ua
Контактний телефон	заповнюється за домовленістю
Сторінка дисципліни в ІСУ	https://msn.khmnu.edu.ua/course/view.php?id=7743
Навчальний рік	2024/2025
Консультації	Онлайн: за необхідністю та попередньою домовленістю

Характеристика дисципліни

Форма навчання	Курс	Семестр	Загальне навантаження		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, в т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	1	парний	8	240	108	36	36	36		132			+	
Разом ДФН			**8**	**240**	**108**	**36**	**36**	**36**		**132**			**1**	

Анотація дисципліни

Дисципліна "Криптологія" є однією із вибіркових дисциплін загальної підготовки бакалаврів галузі інформаційних технологій.

Дисципліна викладається для здобувачів першого (бакалаврського) рівня вищої освіти денної форми навчання спеціальностей «Комп'ютерна інженерія», «Інформаційні системи та технології». При викладанні дисципліни використовуються активні і творчі форми проведення занять, зокрема, методи проблемного навчання.

Розробник: к.т.н., доц., Капустян М.В.

Погоджено:

Зав. каф. КІІС: к.т.н., доц. Засорнова І.О.

Гарант ОПП «КІП»: д.т.н., проф. Лисенко С.М.

Мета і завдання дисципліни

Метою дисципліни "Криптологія" є освоєння студентами теоретичних і практичних основ криптології, криптографії та принципів розробки програмного забезпечення для їх реалізації на робочих станціях.

Завдання дисципліни. Надати студентам знання і практичні навички із використання криптології в комп'ютерних системах та мережах.

Очікувані результати навчання.

Студент, який успішно завершив вивчення дисципліни, повинен: вміло *використовувати* набуті знання зі стандартів інформаційної безпеки, основних методів та засобів захисту; *виконувати* основні задачі із забезпечення захисту інформації; *демонструвати* практичні навички із застосування криптографічних засобів захисту; *аналізувати* стан інформаційної безпеки та *визначати* причини появи каналів витоку інформації.

Компетентності, на формування яких спрямовано ОК:

Інтегральна – Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю та невизначеністю умов

ЗК2 – Здатність вчитися і оволодівати сучасними знаннями

ЗК3 – Здатність застосовувати знання у практичних ситуаціях

ЗК4 – Здатність спілкуватися державною мовою як усно, так і письмово

ЗК7 – Вміння виявляти, ставити та вирішувати проблеми

ЗК11 – Здатність до розуміння предметної галузі та професійної діяльності.

ЗК12 – Здатність використовувати інформаційні та комунікаційні технології

ЗК13 – Здатність розв'язувати поставлені задачі та приймати відповідні рішення

ФК1 – Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії

ФК7 – Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності

ФК9 – Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи

ФК13 – Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій

ФК16 – Здатність до аналізу, синтезу і оптимізації комп'ютерних та інформаційних технологій з використанням математичних моделей і методів

ФК20 – Здатність використовувати та керувати сучасними інформаційними технологіями, технологіями комп'ютерної інженерії, методиками й техніками кібербезпеки під час виконання функціональних завдань та обов'язків

Програмні результати навчання, на забезпечення яких спрямовано ОК:

ПРН3 – Знати новітні технології в галузі комп'ютерної інженерії

ПРН6 – Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей

ПРН11 – Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії

ПРН15 – Вміти виконувати експериментальні дослідження за професійною тематикою

ПРН17 – Спілкуватись усно та письмово з професійних питань українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською)

ПРН18 – Використовувати інформаційні технології для ефективного спілкування на професійному та соціальному рівнях

ПРН19 – Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення

ПРН20 – Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення

ПРН21 – Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики

ПРН23 – Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із

застосуванням об’єктно-орієнтованого програмування для розв’язання задач проектування і використання програмно-технічних засобів комп’ютерних систем та мереж

ПРН25 – Адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та технології комп’ютерної інженерії із забезпеченням захисту інформації в комп’ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки

Тематичний і календарний план вивчення дисципліни

Номер лекції	Перелік тем лекцій	Кількість годин
	Парний семестр	
1	Елементарна криптологія	2
2	Шифри з використанням булевої алгебри	2
3	Математичні основи криптографії	4
4	Афінні шифри	2
5	Арифметичні задачі та алгоритми	4
6	Факторизація. Розпізнавання квадратичності і добування квадратних коренів.	4
7	Криптосистеми з відкритим ключем	2
8	Генератори псевдовипадкових бітів	4
9	Важкооборотні функції	4
10	Цифровий підпис	4
11	Адміністрування ключами	4
Разом за восьмий семестр:		**36**

Примітка: *Лекції проводяться кожного тижня по дві години; послідовність проведення занять визначається розкладом (може не відповідати нумерованим тижням)

Політика дисципліни

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов’язаний відвідувати лекції та лабораторні заняття згідно з розкладом, не запізнюватися на заняття, завдання виконувати відповідно до графіка. Пропущене лабораторне заняття студент зобов’язаний опрацювати самостійно у повному обсязі і відзвітувати перед викладачем не пізніше, ніж за тиждень до чергової атестації. До лабораторних занять студент має підготуватися за відповідною темою і проявляти активність. Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання у ХНУ.

Критерії оцінювання результатів навчання

Кожний вид роботи з дисципліни оцінюється за ***чотирибальною*** шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з врахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих її видів робіт. При оцінюванні знань студентів використовуються різні засоби контролю, зокрема: усне опитування перед допуском до виконання лабораторної роботи – здійснюється на їх початку; якість виконання, набуття теоретичних знань і практичних навичок перевіряється шляхом захисту кожної лабораторної роботи згідно з робочою програмою дисципліни і робочим навчальним планом.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів денної форми навчання у семестрі за ваговими коефіцієнтами

Аудиторна робота								Семестр. контроль (залік)
І семестр								
Лабораторні роботи №:								Залік за рейтингом
1	2	3	4	5	6	7	8	
ВК:				1				

Умовні позначення: ВК – ваговий коефіцієнт.

Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ECTS	**Інституційна шкала балів**	**Інституційна оцінка**		**Критерії оцінювання**
A	4,75-5,00	5	Зараховано	**Відмінно** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків.
B	4,25-4,74	4		**Добре** – повне знання навчального матеріалу з кількома незначними помилками.
C	3,75-4,24	4		**Добре** – в загальному правильна відповідь з двома-трьома суттєвими помилками.
D	3,25-3,74	3		**Задовільно** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією.
E	3.00-3,24	3		**Задовільно** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00-2,99	2	Незараховано	**Незадовільно** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00-1,99	2		**Незадовільно** – необхідна серйозна подальша робота і повторне вивчення дисципліни.

Питання для підсумкового контролю з дисципліни

1. Шифр простої заміни.
2. Частотний аналіз.
3. Гомофонний шифр заміни.
4. Поліграмні шифри.
5. Поліалфавітні шифри.
6. Шифри перестановок.
7. Шифр одноразового блокноту.
8. Композиція (добуток) шифрів.
9. Криптосистема DES.
10. Модифікації блокових шифрів.
11. Дешифрування ітераціями.
12. Алгоритм Евкліда.
13. Конгруенції. Кільце лишків. Кільце матриць
14. Бінарний метод піднесення до степеня.
15. Випадковий вибір.
16. Первісні корені. Квадратичні лишки. Символ Якобі.
17. Розподіл простих чисел. Ймовірносний тест Соловея-Штрассена.
18. Псевдопрості числа.
19. Ймовірносний тест Міллера-Рабіна.
20. Розпізнавання квадратичності і добування квадратних коренів.
21. Криптосистема RSA.

22. Криптосистема Рабіна.
23. Криптосистема Ель-Гамаля.
24. Ймовірносне криптування.
25. Криптосистеми на основі еліптичних кривих.
26. Генератори псевдовипадкових бітів.
27. Важкооборотні функції.
28. Цифровий підпис.
29. Адміністрування ключами.
30. Криптостійкість засобів ЕЦП.
31. Поняття електронного сертифікату.
32. Моделі систем сертифікації.
33. Проблеми та перспективи впровадження ЕЦП в Україні.
34. Правове регулювання ЕЦП в Україні та світі.
35. Алгоритм цифрового підпису Шнорра.
36. Сліпий підпис, незаперечний підпис, груповий підпис.
37. Криптографічні протоколи
38. Вимоги до протоколів автентифікації.
39. Модель загроз порушення автентичності.
40. Модель взаємної недовіри та взаємного захисту.
41. Основи криптографії на еліптичних кривих
42. Алгоритм обчислення порядку еліптичної кривої.
43. Криптосистема Мессі-Омури над групою точок еліптичної кривої.
44. Аналіз вразливостей криптографічної схеми цифрового підпису ECDSA.
45. Елементи криптоаналізу шифрів
46. Силові методи криптоаналізу.
47. Криптоаналіз по побічним каналам.
48. Нові напрямки в криптографії
49. Стеганографія та її застосування.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни забезпечений необхідними навчально-методичними розробками в модульному середовищі.

Розробник: к.т.н., доц., Капустян М.В.

Погоджено:

Зав. каф. КІІС: к.т.н., доц. Засорнова І.О.