



**Міжнародний гуманітарний університет
ФАХОВИЙ КОЛЕДЖ
Циклова комісія зі спеціальності «Комп'ютерна інженерія»**

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КРИПТОГРАФІЇ

Галузь знань	12 – «Інформаційні технології»
Спеціальність	123 – «Комп'ютерна інженерія»
Назва освітньої програми	Комп'ютерна інженерія
Рівень передвищої освіти	Фаховий передвищий рівень

Розробники і викладачі	Контактний тел.	E-mail
кандидат технічних наук, доцент Йона Лариса Григорівна	+380677463777	yonalarysa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Дисципліна Основи криптографії є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 123 «Комп'ютерна інженерія», а також обов'язковим компонентом освітньої програми для здобуття фахового передвищого освітнього рівня. Вона формує у здобувачів уявлення про принципи криптографічного захисту інформації та запобігання втрати властивостей у інформації, що захищається.

Метою викладання навчальної дисципліни «Основи криптографії» є забезпечення здобувачів знаннями з питань захисту інформації методами криптографічного перетворення та принципів побудови криптографічних систем.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ, ТА ДОСЯГНЕННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Інтегральна компетентність	
ІК	Здатність вирішувати типові спеціалізовані задачі в галузі інформаційних технологій в процесі професійної діяльності або навчання, що вимагає застосування методів і технологій комп'ютерної інженерії та може характеризуватися певною невизначеністю умов; нести відповідальність за результати своєї діяльності, здійснювати контроль інших осіб у визначених ситуаціях
Загальні компетентності	
ЗК4	Здатність застосовувати знання у практичних ситуаціях
ЗК8	Здатність вчитися і оволодівати сучасними знаннями
Спеціальні (фахові) компетентності	
СК1	Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційних технологій
СК5	Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки
СК6	Здатність брати участь у модернізації апаратних та програмних засобів комп'ютерної інженерії
СК7	Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи
СК10	Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення
СК12	Здатність створювати, впроваджувати, адмініструвати бази даних і знань з використанням сучасних методів, технологій та систем керування базами даних
СК14	Здатність оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності
СК15	Здатність оцінювати рівень захисту інформації в комп'ютерних засобах та системах і обґрунтовувати вибір апаратних та програмних засобів для забезпечення його належного рівня
Програмні результати навчання	
РН2	Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії
РН3	Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії
РН9	Розробляти, тестувати, впроваджувати, експлуатувати програмне забезпечення для вбудованих і розподілених систем
РН11	Ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів комп'ютерної інженерії
РН15	Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки
РН17	Обґрунтовано обирати та використовувати методи криптографії для забезпечення необхідного рівня захисту інформації в комп'ютерних системах та мережах

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття			Ознаки курсу		
ЄКТС	годин	Лекційні заняття	Практичні заняття	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
5	150	28	56	66	4 (на основі БЗСО) 3 (на основі ПЗСО)	7 (на основі БЗСО) 5 (на основі ПЗСО)	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин			
	Загалом	Лекційні заняття	Практичні заняття	Самостійна робота
Змістовий модуль 1. Класичні методи шифрування				
Тема 1. Розвинення криптографії та її місце в сучасному суспільстві.	10	2	4	4
Тема 2. Класичні методи шифрування. Класифікація шифрів. Шифри перестановки. Шифри простої та складної заміни. Шифри гамування. Роторні машини.	10	2	4	4
Тема 3. Засади криптографічного захисту інформації. Завдання, що розв'язуються криптографічними методами. Вимоги до реалізації сучасних алгоритмів.	10	2	4	4
Тема 4. Засади криптографічного захисту інформації. Завдання, що розв'язуються криптографічними методами. Вимоги до реалізації сучасних алгоритмів.	10	2	4	4
Тема 5. Поточні шифри . Шифри гамування. Накладання гами шифру на відкритий текст. Методи генерування псевдовипадкової послідовності чисел.	10	2	4	4
Змістовий модуль 2 . Принципи побудови криптосистем.				
Тема 6. Поняття криптосистеми. Типи криптосистем. Класифікація криптосистем за призначенням.	10	2	4	4
Тема 7. Класичні симетричні криптосистеми. Принципи побудови симетричних криптосистем. Порівняльний аналіз симетричних криптосистем.	10	2	4	4
Тема 8. Концепція криптосистеми з відкритим ключем. Однонаправлені геш-функції.	10	2	4	4
Тема 9. Принципи керування ключовою системою.	10	2	4	4
Тема 10. Асиметричні алгоритми шифрування. Процедури шифрування в асиметричних криптосистемах. Порівняльний аналіз асиметричних криптосистем.	12	2	4	6
Тема 11. Системи ідентифікації та автентифікації. Поняття багатофакторної автентифікації.	12	2	4	6

Тема 12. Методи побудови схем електронного підпису. Різновиди схем електронного підпису.	12	2	4	6
Тема 13. Основи побудови криптосистем на еліптичних кривих.	12	2	4	6
Тема 14. Методи та інструменти захисту інформації в мережі Internet з використанням технології Blockchain.	12	2	4	6
Загалом	150	28	56	66
Підсумковий контроль – екзамен				

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom. Виконання практичних робіт та проведення індивідуального тестування, забезпечується за допомогою існуючих в університеті комп'ютерних класів, бібліотеки та платформ он-лайн навчання на основі інформаційних систем Moodle або Google Classroom.

6. САМОСТІЙНА РОБОТА

№ з/п	Назва теми	Кількість годин
1	Тема 1. Розвинення криптографії. Дослідження етапів удосконалення шифрів.	4
2	Тема 2. Класичні методи шифрування. Шифри перестановки. Практичне використання шифрів перестановки у системах зв'язку.	4
3	Тема 3. Принципи побудови секретної системи зв'язку.	4
4	Тема 4. Модифікована мережа Файстеля. SP-мережа.	4
5	Тема 5. Шифр Вернама.	4
6	Тема 6. Симетричні криптосистеми. Режим роботи та функціональні перетворення.	4
7	Тема 7. Реалізація SP-мережі в криптосистемах AES та ДСТУ 7624:2014 «Калина».	4
8	Тема 8. Вимоги до несиметричних криптосистем.	4
9	Тема 9. Ключова система, генерування та розподілення ключів	4
10	Тема 10. Особливості побудови систем з відкритим ключем.	6
11	Тема 11. Процедури шифрування в криптосистемі Ель–Гамала.	6
12	Тема 12. Прості методи автентифікації за паролем.	6
13	Тема 13. Класифікація атак на схеми електронного підпису.	6
14	Тема 14. Захист інформації в технології Blockchain.	6
	Загалом	66

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль та тестування, які здійснюються у ході проведення практичних занять, консультацій та відпрацювань		50%
Підсумковий контроль, який здійснюється у ході проведення екзамену		50%
Методи діагностики знань (контролю)	Фронтальне опитування, тестові завдання, робота у групах, розв'язання практичних завдань, екзамену	

8. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

Поточний контроль			
Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	20
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування	Відповідно до робочої програми та розкладу занять	Перевірка результатів виконання тесту	20
Виконання індивідуальних завдань (науково-дослідна робота здобувача)			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів.	10
Загалом балів за поточний контроль			50
Підсумковий контроль – екзамен			50
Загалом балів			100

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ

Рівень знань оцінюється:

– «відмінно» / «зараховано» А – від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, на екзамені демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставлені завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» В – від 82 до 89 балів. Здобувач володіє знаннями матеріалу на екзамені, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях, практичних та лабораторних заняттях, під час яких виконував усі поставлені завдання та давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, виконав лабораторні роботи та завдання до самостійної роботи, проявляє активність і творчість у науково-дослідній роботі;

– «добре» / «зараховано» С – від 74 до 81 балів. Здобувач відтворює значну частину теоретичного матеріалу на екзамені, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи та активність у науково-дослідній роботі;

– «задовільно» / «зараховано» D - від 64 до 73 балів. Здобувач був присутній не на всіх лекціях та практичних заняттях, на екзамені володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність виконаних лабораторних робіт та завдань до самостійної роботи;

– «задовільно» / «зараховано» E – від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та практичних заняттях, на екзамені володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, виконав не всі завдання до самостійної роботи;

– «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;

– «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів. Здобувач не володіє навчальним матеріалом.

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	Зараховано
74-81	C		
64-73	D		
60-63	E	Задовільно	Зараховано
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Стрелковська І.В. Вища математика для фахівців в галузі зв'язку. Ч.5 / І.В. Стрелковська, В.М. Паскаленко. – Одеса: ВМВ, 2018. – 508 с.
2. Стрелковська І.В. Диференціальні рівняння для фахівців в галузі ІТ-галузі / І.В. Стрелковська, В.М. Паскаленко. – Одеса: ОНАЗ, 2018. – 188 с.
3. Чисельні методи: Навчальний посібник. / Волонтир Л.О, Зелінська О.В., Потапова Н.А., Чіков І.А., Вінницький національний аграрний університет. – Вінниця: ВНАУ, 2020 – 322 с.
4. Крилик Л. В. Обчислювальна математика. Інтерполяція та апроксимація табличних даних: навчальний посібник / Л. В. Крилик, І. В. Богач, М. О. Прокопова. – Вінниця : ВНТУ, 2013. – 111 с.
5. Нещадим О.М., Панкрат'єв В.О. Чисельні методи: Методичні вказівки до виконання лабораторних робіт для студентів ОС "Бакалавр" спеціальності 122 "Комп'ютерні науки" денної форми навчання.– К.: ЦП "КОМПРИНТ", 2019. – 96 с.
6. Задачин В.М., Конюшенко І.Г. Чисельні методи: Навчальний посібник. Вид. ХНЕУ ім. С. Кузнеця, 2014. 180 с.
7. Панкрат'єв В.О., Шукайло Є.М. Чисельні методи в інформатиці: Методичні вказівки до виконання лабораторних робіт для студентів напряму підготовки "Комп'ютерні науки" денної форми навчання.– К.: ВЦ НУБіП, 2011. – 76 с.

Допоміжна

8. Стрелковська І.В. Теорія ймовірностей та випадкові процеси (для фахівців у галузі ІТ-технологій) / І.В. Стрелковська, В.М. Паскаленко. – Одеса: ОНАЗ, 2018. – 384 с.
9. Стрелковська І.В. Математична статистика / І.В. Стрелковська, В.М. Паскаленко. – Одеса: ОНАЗ, 2019. – 110 с.
10. Лук'яненко С.О. Числові методи в інформатиці: навч. посіб. / – Вид. 2-ге, доп. та випр. – К.: НТУУ "КПІ", 2012. – 160 с.
11. Крижанівська Т.В., Бойцова І.А. Конспект лекцій з дисципліни „Чисельні методи”. Одеса, 2013. – 152 с.
12. Математичні методи моделювання : навчальний посібник / О. П. Чорний, В. К. Титюк, Н. М. Істоміна та ін. ; заг. ред. О. П. Чорний. – Кременчук : ПП Щербатих О. В., 2016. – 232 с.

Інформаційні ресурси

13. Чисельні методи в інформатиці [Електроний ресурс]: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/16377/1/%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BA%D0%B0%20%D1%87%D0%B8%D1%81%D0%B5%D0%BB%D1%8C%D0%BD%D1%96%20%D0%BC%D0%B5%D1%82.pdf>
14. <https://probability.knu.ua/tims/>
15. <https://www.ams.org/publications/journals/journalsframework/tpms>