ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптологія

Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 9 кредитів ЄКТС
Шифр дисципліни – ОПП.09
Мова навчання – Українська
Статус дисципліни – Обов'язкова (професійної підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	2	4	4	120	50	16	34	-	-	70	-	-	-	+
Д	3	5	5	150	50	16	34	-	-	100	-	-	-	+
Разом ДФН			**9**	**270**	**100**	**32**	**68**	**-**	**-**	**170**	**-**	**-**	**-**	**2**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю 125 «Кібербезпека та захист інформації»

Робоча програма складена _____ Володимир АНІКІН
Підпис автора(ів) канд. техн. наук, доцент Юрій КЛЬОЦ
Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

ВСТУП

Дисципліна «Прикладна криптологія» - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека».

Пререквізити – ОПП.03 Математичні основи захисту інформації, ОПП.04 Теорія інформації та кодування.

Постреквізити – ОПП.15 Виробнича практика 1, ОПП.16 Виробнича практика 2.

***компетентності*:**

ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ФК 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

ФК 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

результати навчання:

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації.

ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах

Метою викладання навчальної дисципліни є формування у майбутніх спеціалістів умінь та компетенцій для ефективного застосування методів та засобів криптографічного захисту інформації на об'єктах інформаційної діяльності; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Предметом дисципліни є методи та засоби криптографічного захисту інформації; методи та засоби криптоаналізу; сучасне програмно-апаратне забезпечення криптографічного захисту інформаційно-комунікаційних технологій та систем.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека та захист інформації»:

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* теорії та методи криптографічного захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації; *виконувати* впровадження та підтримку компонентів криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *адаптуватися* в умовах частої зміни технологій професійної діяльності та *прогнозувати* кінцевий результат при вирішенні практичних задач криптографічного захисту інформації.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

IV семестр

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Класична криптографія та криптоаналіз	4	8	24
Тема 2. Сучасні симетричні криптосистеми та їх криптоаналіз	8	16	28
Тема 3. Автентифікація та хешування	4	10	18
Разом:	**16**	**34**	**70**

V семестр

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Асиметричні криптосистеми та їх криптоаналіз	6	12	36
Тема 2. Цифрові підписи та криптографічні сертифікати	6	12	36
Тема 3. Постквантова криптографія	2	4	12
Тема 4. Основи цифрової стеганографії	2	6	16
Разом:	**16**	**34**	**100**

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу (IV семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Класична криптографія та криптоаналіз		
1	**Вступ до криптології. Класична криптографія давніх часів та її криптоаналіз** 1. Поняття криптології, її мета, предмет та об'єкт. Складові криптології. Історія розвитку криптографії та криптоаналізу. 2. Шифри простої моноалфавітної заміни. 3. Шифри перестановки. 4. Гомофонний шифр заміни. 5. Поліграмні шифри. [1] с. 13-78, [2] с. 8-16, [3] с. 6-24, [4] с. 13-18	2
2	**Криптографія доцифрової епохи та її криптоаналіз** 1. Поліалфавітні шифри. Шифр Віженера. 2. Роторні шифрувальні машини. Машина «Енігма» та її криптоаналіз. 3. Афінні шифри. 4. Шифр одноразових блокнотів. [1] с. 78-191, [3] с. 24-29, [4] с. 18-26	2
Тема 2. Сучасні симетричні криптосистеми та їх криптоаналіз		
3	**Випадкові числа. Криптографічна стійкість** 1. Поняття криптографічної ентропії. 2. Поняття випадкової та псевдовипадкової генерації. 3. Вимоги до криптостійкого генератора псевдовипадкових чисел. 4. Криптографічно стійкі алгоритми генерації псевдовипадкових чисел. Алгоритм Блюм-Блюм-Шуба. 5. Стандарт ДСТУ ISO/IEC 18031:2015. [2] с. 16-45	2
4	**Симетричні потокові шифри та їх вразливості** 1. Ранні потокові симетричні криптосистеми та їх вразливості. 2. Вимоги до стійкості сучасних симетричних потокових криптосистем. 3. Криптосистема Salsa20. 4. Вітчизняний стандарт ДСТУ 8845:2019 «СТРУМОК» [2] с. 324-326, [3] с. 29-33, [4] с. 33-42	2
5	**Симетричні блокові шифри та їх вразливості** 1. Перші блокові симетричні шифри. Мережа Фейстеля. 2. Застарілий стандарт блокового шифрування DES та його модифікації. 3. Стандарт блокового шифрування AES. 4. Вітчизняний стандарт ДСТУ 7624:2014 «Калина» 5. Криптоаналіз сучасних блокових криптосистем. Лінійний та диференційний криптоаналіз. [2] с. 226-240, [3] с. 33-42, [4] с. 42-70	2
6	**Режими роботи симетричних блокових шифрів** 1. Поняття режиму шифрування. Режим ECB як приклад вразливого застосування стійких шифрів. 2. Режими CBC, CFB, OFB та інші режими ланцюгування. 3. Режим CTR. Перетворення блокового шифрування в потокове. 4. Режим XTS. Проблематика шифрування жорстких дисків [2] с. 340-359, [3] с. 46-50	2

Тема 3. Автентифікація та хешування		
7	**Криптографічні функції хешування** 1. Поняття криптографічного хешування та вимоги до його стійкості. 2. Основні типи будови криптографічних функцій хешування. Компресійна конструкція та конструкція криптографічної губки. 3. Сімейство функцій хешування MD. 4. Сімейство функцій хешування SHA-2 та SHA-3. 5. Вітчизняний стандарт хешування ДСТУ 7564:2014. 6. Хешування паролів. Методи хешування із доданою складністю. [3] с. 59-64, [4] с. 86-93	2
8	**Криптографічна автентифікація та автентифіковані режими симетричного шифрування** 1. Вразливості не автентифікованого шифрування. 2. MDC та MAC. 3. Схеми верифікації не автентифікованих режимів шифрування. 4. Автентифіковані режими шифрування. Режим GCM та GCM-SIV. [2] с. 483-551	2
	Разом за семестр:	**16**

Зміст лекційного курсу (V семестр)

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Асиметричні криптосистеми та їх криптоаналіз		
1	**Поняття асиметричної криптографії. Протоколи узгодження ключів.** 1. Криптографічні односторонні функції. Математичне обґрунтування їх функціонування. 2. Модульна арифметика в асиметричній криптографії. 3. Анонімний протокол Діффі-Геллмана. 4. Автентифікований протокол Діффі-Геллмана. [2] с. 403-410, [3] с. 42-43	2
2	**Асиметричні криптосистеми та механізми їх роботи. Криптосистема RSA** 1. Варіанти побудови асиметричних криптосистем. 2. Криптосистема Ель-Гамаля. Криптосистема Рабіна. 3. Розширений алгоритм Евкліда. 4. Криптосистема RSA. Правила генерації ключів. 5. Вразливості криптосистеми RSA. Криптоаналіз RSA. [2] с. 410-423, [3] с. 42-46, [4] с. 76-84	2
3	**Асиметричні криптосистеми на основі операцій на еліптичних кривих** 1. Поняття групи у абстрактній алгебрі. Вимоги до групи. 2. Правила проведення операцій на еліптичних кривих. 3. Вимоги до параметрів кривої. Умови стійкості операцій на кривих 3. Протокол Діффі-Гелмана на еліптичних кривих. 4. Протокол Ель-Гамаля на еліптичних кривих. [2] с. 459-483, [4] с. 97-105	2
Тема 2. Цифрові підписи та криптографічні сертифікати		
4	**Поняття цифрового підпису та можливості його реалізації методами асиметричної криптографії** 1. Мета та проблематика цифрових підписів. 2. Використання криптосистеми RSA для реалізації цифрових підписів. 3. Вразливості підпису RSA. Атака Блейхенбахера.	2

	4. Цифровий підпис RSA-PSS. 5. Алгоритми цифрового підпису DSA та ECDSA. [2] с. 483-551	
5	**Стандарти цифрових підписів** 1. Нормативно-правове регулювання цифрових підписів в Україні. 2. Вітчизняні стандарти КЕП. Стандарт ДСТУ 4145. 3. Міжнародні стандарти цифрового підпису. [4] с. 93-97	2
6	**Інфраструктура публічних ключів. Основи протоколу TLS** 1. Загальна структура протоколів TLS. Протокол TLS 1.3. 2. Поняття сертифікату. Структура інфраструктури публічних ключів. 3. Стандарт сертифікатів X.509. Розширення сертифікатів. 4. Життєві цикли сертифікатів. Процес сертифікації. 5. Інструменти бібліотеки OpenSsl. [3] с. 56-68	2
Тема 3. Постквантова криптографія		
7	**Загрози квантової криптографії та шляхи їх усунення** 1. Теорія квантової криптографії. Потенційний квантовий криптоаналіз. 2. Алгоритм Шора. 3. Алгоритм Гровера. 4. Методи превентивної протидії загрозам квантового криптоаналізу. [2] с. 553-632	2
Тема 4. Основи цифрової стеганографії		
8	**Основи цифрової стеганографії** 1. Стеганографічні системи. Модель та основні вимоги. Відкриті, закриті та напівзакриті стеганосистеми. 2. Атаки на стеганографічні системи та протидія їм. 3. Пропускна здатність каналів приховуваної передачі повідомлень. 4. Оцінювання стійкості стеганографічних систем. [1] с. 755-789	2
	Разом за семестр:	**16**

Зміст лабораторних робіт (IV семестр)

№ п/п	Теми лабораторних робіт	Кількість годин
1	Класичні шифри перестановки, полігамні шифри та їх криптоаналіз	4
2	Класичні шифри підстановки та їх криптоаналіз	4
3	Дослідження генераторів псевдовипадкових чисел	4
4	Вразливості симетричних потокових шифрів	4
5	Симетричні блокові шифри. Лінійний криптоаналіз	4
6	Вразливості режимів симетричного шифрування	4
7	Методи криптографічного хешування та їх вразливості	4
8	Застосування методів криптографічної автентифікації	4
9	Підсумкове заняття. Контрольна робота	2
	Разом за семестр:	**34**

Зміст лабораторних робіт (V семестр)

№ п/п	Теми лабораторних робіт	Кількість годин
1	Протокол узгодження ключів Діффі-Геллмана	4
2	Криптосистема RSA та її вразливості	4
3	Криптосистеми на еліптичних кривих	4
4	Застосування асиметричних криптосистем у режиму підпису.	4
5	Цифровий підпис та можливості його компрометації	4
6	Створення та використання криптографічних сертифікатів в інфраструктурі публічних ключів	4
7	Загрози квантової криптографії та шляхи їх усунення	4
8	Цифрові водяні знаки та інше прикладне застосування цифрової стеганографії	4
9	Підсумкове заняття. Контрольна робота	2
	Разом за семестр:	**34**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни становить 170 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи (IV семестр)	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	3
2	Підготовка до виконання лабораторної роботи №1	3
3	Опрацювання теоретичного матеріалу лекції №2.	3
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	5
5	Підготовка до тестування за темою №1. Опрацювання теоретичного матеріалу лекції №3.	4
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	5
7	Опрацювання теоретичного матеріалу лекції №4.	3
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	5
9	Опрацювання теоретичного матеріалу лекції №5.	3
10	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	5
11	Опрацювання теоретичного матеріалу лекції №6.	3
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	5
13	Опрацювання теоретичного матеріалу лекції №7.	3
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	5
15	Опрацювання теоретичного матеріалу лекції №8.	3
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	5
17	Підготовка до захисту лабораторної роботи №8.	3
18	Підготовка до контрольної роботи за пройденим матеріалом.	4
	Разом за семестр:	70

№ тижня	Теми самостійної роботи (V семестр)	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	6
2	Підготовка до виконання лабораторної роботи №1	5
3	Опрацювання теоретичного матеріалу лекції №2.	5
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6
5	Опрацювання теоретичного матеріалу лекції №3.	5
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6
7	Підготовка до тестування за темою №1. Опрацювання теоретичного матеріалу лекції №4.	5
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6
9	Опрацювання теоретичного матеріалу лекції №5.	5
10	Підготовка до захисту лабораторної роботи №4. Підготовка до	6

	виконання лабораторної роботи №5.	
11	Опрацювання теоретичного матеріалу лекції №6.	5
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6
13	Підготовка до тестування за темою №2. Опрацювання теоретичного матеріалу лекції №7.	5
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6
15	Опрацювання теоретичного матеріалу лекції №8.	5
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6
17	Підготовка до захисту лабораторної роботи №8.	4
18	Підготовка до контрольної роботи за пройденим матеріалом.	8
	Разом за семестр:	100

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій, зокрема: лекції (з використанням методів проблемного навчання і візуалізації); лабораторні роботи (бесіда, демонстрування, спостереження, з використанням кейсів, розв'язування задач, презентацій), самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання лабораторних робіт).

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів навчання, зокрема: методи навчання за джерелом передачі і сприймання інформації (словесні (пояснення, дискусія, консультування), практичні (інструктування, розв'язування ситуаційних задач), наочні (демонстрування, ілюстрування, спостереження); за логікою передачі і сприймання навчальної інформації; за рівнем самостійності пізнавальної діяльності (методи проблемного викладу, частково пошукові, дослідницькі); методи стимулювання і мотивації учіння, інтерактивні; метод аналізу конкретних ситуацій (case-study) з використанням технологій візуалізації, інформаційно-комунікаційних та технології дистанційного навчання (сервіс для проведення онлайн конференцій Zoom, Модульне середовище для навчання тощо).Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції пояснювально-ілюстративними та проблемними методами з супроводом презентаційних матеріалів, лабораторні роботи проводяться з використанням практичних, продуктивних, проблемних та контекстних методів, із застосуванням методів моделювання та сучасних інформаційно-комп'ютерних технологій і мають за мету – формування у майбутніх спеціалістів умінь та компетенцій для ефективного застосування методів та засобів криптографічного захисту інформації на об'єктах інформаційної діяльності; розвиток у студентів фахового стилю мислення; надання глибоких та міцних знань з питань криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час захистів звітів лабораторних робіт, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу.

При цьому використовуються такі методи поточного контролю:

– усне опитування;

– тестовий контроль теоретичного матеріалу;

– оцінювання звітів лабораторних робіт.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, не допускається до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який має академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

ПОЛІТИКА ДИСЦИПЛІНИ

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, проходження інструктажу з техніки

безпеки; відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в індивідуальному режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до лабораторних робіт (вивчення теоретичного матеріалу з теми, активно працювати на занятті, розв'язувати задачі, брати участь у дискусіях щодо прийнятих рішень при виконанні здобувачами задач).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Пропущену лабораторну роботу здобувач зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами захисту звітів лабораторних робіт та тестування.

Здобувач вищої освіти, виконуючи самостійну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, підказки, плагіат, використання штучного інтелекту (без вірного цитування)). У разі порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності під час вивчення навчальної дисципліни не допускаються та не толеруються.

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах (https://7eminar.ua/, https://seminar.expertus.com.ua/, https://sys2biz.com.ua/seminars/, https://finacademy.net/ua/webinars), які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із призначених робочою програмою для цього виду роботи. При цьому кожна структурна одиниця (робота) може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

Будь-які форми порушення академічної доброчесності не допускаються та не толеруються.

Отриманий здобувачем бал за зарахований вид навчальної роботи (структурну одиницю) після її оцінювання викладач виставляє в електронному журналі обліку успішності здобувачів вищої освіти. За умови виконання усіх видів навчальної роботи за результатами поточного контролю протягом вивчення навчальної дисципліни, встановлених її Робочою програмою, здобувач денної форми здобуття освіти з навчальної дисципліни, підсумковим контролем для якої є іспит, може набрати до 60 балів (здобувач заочної форми – до 50 балів). Позитивну підсумкову оцінку здобувач може отримати, якщо за результатами поточного та підсумкового контролів набере від 60 до 100 балів. Семестрова підсумкова оцінка розраховується в автоматизованому режимі в інформаційній підсистемі «Електронний журнал» (ІС «Електронний університет») і відповідно до накопиченої суми балів визначається оцінка за інституційною шкалою та шкалою ЄКТС (див. таблицю Співвідношення…), яка заноситься в екзаменаційну відомість, а також до Індивідуального навчального плану здобувача вищої освіти.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів *денної* форми здобуття освіти у 4 семестрі

Аудиторна робота								**Контрольні заходи**		**Семестро-вий контроль**	**Разом**
Четвертий семестр											Сума балів
Лабораторні роботи								Тестовий контроль:		Іспит	
1	2	3	4	5	6	7	8	Т*1	Т*2-3		
Кількість балів за вид навчальної роботи (мінімум-максимум)											
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	6-10	6-10	24-40	
24-40								**12-20**		**24-40**	**60-100****

Примітка : **Т*** – тема навчальної дисципліни;

За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів *денної* форми здобуття освіти у 5 семестрі

Аудиторна робота								**Контрольні заходи**		**Семестро-вий контроль**	**Разом**
П'ятий семестр											Сума балів
Лабораторні роботи								Тестовий контроль:		Іспит	
1	2	3	4	5	6	7	8	Т*1	Т*2		
Кількість балів за вид навчальної роботи (мінімум-максимум)											
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	6-10	6-10	24-40	
24-40								**12-20**		**24-40**	**60-100****

Примітка : **Т*** – тема навчальної дисципліни;

За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання лабораторних робіт

Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: оцінка, отримана за захист звітів відповідної за номером та темою лабораторної роботи; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення. Пропущене заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі. Оцінку за лабораторну

роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

При оцінюванні результатів навчання здобувачів вищої освіти на лабораторних роботах викладач користується наведеними нижче критеріями:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі), демонструє якісне оформлення завдань, вміє заповнювати форми звітності, аналізувати їх на помилки та виправляти їх, шукати взаємозв'язки між формами. Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Оцінювання результатів тестового контролю

Кожен з двох тестів, передбачених робочою програмою, складається із 40 тестових завдань. Максимальна сума балів, яку може набрати студент за результатами тестування, складає 10.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 6 до 10 балів:

Таблиця – Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	1-23	24-26	27-29	30-32	33-35	36-40
Відсоток правильних відповідей	0-59	60-67	68-75	76-83	84-91	92-100
Кількість балів	-	6	7	8	9	10

На тестування відводиться 30 хвилин. Правильні відповіді студент записує у талоні відповідей. Студент може також пройти тестування і в онлайн режимі у Модульному середовищі для навчання на сторінці навчальної дисципліни. Тестування здобувачів вищої освіти у Модульному середовищі для навчання автоматично оцінюються за критеріями, наведеними у таблиці вище.

При отриманні негативної оцінки тест слід перездати до терміну наступного контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного (в т.ч. у тестовій формі), так і практичного характеру.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми здобуття освіти (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Практичне завдання	12	16	20
Разом:	**24**		**40**

***Примітка**. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.*

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

<table>
<tr><th rowspan="2">Оцінка ЄКТС</th><th rowspan="2">Рейтингова шкала балів</th><th colspan="2">Інституційна шкала (Опис рівня досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни</th></tr>
<tr><th>Залік</th><th>Іспит/диференційований залік</th></tr>
<tr><td>A</td><td>90-100</td><td rowspan="5">Зараховано</td><td>Відмінно/Excellent – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>B</td><td>83-89</td><td rowspan="2">Добре/Good – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>C</td><td>73-82</td></tr>
<tr><td>D</td><td>66-72</td><td rowspan="2">Задовільно/Satisfactory – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни</td></tr>
<tr><td>E</td><td>60-65</td></tr>
<tr><td>FX</td><td>40-59</td><td rowspan="2">Незараховано</td><td>Незадовільно/Fail – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом</td></tr>
<tr><td>F</td><td>0-39</td><td>Незадовільно/Fail – Результати навчання відсутні</td></tr>
</table>

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній нижче таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного та підсумкового контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка «відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ РЕЗУЛЬТАТІВ НАВЧАННЯ

1. Роль криптографічних протоколів у задачі забезпечення інформаційної безпеки.
2. Основні визначення, використовувані в криптології.
3. Узагальнена схема криптографічної системи.
4. Основи теорії засекреченого зв'язку К. Шеннона.
5. Шифри простої заміни
6. Гомофонний шифр заміни
7. Поліграмні шифри
8. Поліалфавітні шифри
9. Шифри перестановки
10. Багаторазове шифрування
11. Роторні шифрувальні машини
12. Афінні шифри.
13. Шифр гамування
14. Потокові симетричні шифри (A5, RC4, STRUMOK).
15. Синхронні та самосинхронізовані потокові шифри.
16. Блокові симетричні шифри (RC2, RC5, SAFER, FEAL, Blowfish, мережа Фейстеля).
17. Методи компонування сучасних блокових симетричних шифрів.
18. Стандарт DES. Структура алгоритму шифрування даних.
19. Стандарт DES. Режими виконання алгоритму.

20. Симетричний алгоритм IDEA. Структура алгоритму шифрування даних.
21. Симетричний алгоритм IDEA. Безпека та вразливість ключів.
22. Стандарт AES (Rijndael). Структура алгоритму та раундів.
23. Стандарт AES (Rijndael). Алгоритм розгортання ключа для шифрування даних.
24. Стандарт AES (Rijndael). Відмінності шифрування та розширування.
25. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі простої заміни.
26. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі гамування та зі зворотним зв’язком.
27. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі утворення імітовставки.
28. Стандарт блокового симетричного шифрування ДСТУ 7624:2014 «Калина»
29. Основні визначення випадкової послідовності та вимоги до них.
30. Методи і засоби перевірки на випадковість.
31. Конгруентні генератори псевдовипадкових чисел.
32. Генератор Фібоначі.
33. Генератор псевдовипадкових чисел на основі алгоритму BBS.
34. Генератори псевдовипадкових чисел на основі регістрів зсуву зі зворотним зв'язком.
35. Криптографічна система Діффі–Хеллмана
36. Криптографічна система RSA
37. Криптографічна система Ель-Гамаля
38. Типи розкриття
39. Силові методи криптоаналізу
40. Криптоаналіз за побічними каналами
41. Криптоаналіз класичних шифрів.
42. Диференціальний криптографічний аналіз.
43. Лінійний криптографічний аналіз.
44. Властивості симетричності та вразливі ключі.
45. Атака “Квадрат”.
46. Атака методом інтерполяцій.
47. Атака еквівалентних ключів.
48. Методи зламу на дискретному логарифмуванні.
49. Метод “крок немовляти, крок велетня”.
50. Ідентифікація та автентифікація об’єктів
51. Задачі автентифікації у криптографічному захисті інформації
52. Парольна автентифікація. Методи формування стійких паролів
53. Поняття безумовно безпечних кодів автентифікації, теорія Симонсона.
54. Алгоритм MD5
55. Алгоритм SHA
56. Алгоритм SHA3
57. Застосування функції хешування в криптографії
58. Хеш-функції, що використовують симетричні блокові алгоритми
59. Функція хешування “Купина” – національний стандарт України ДСТУ 7564:2014
60. Коди автентифікації повідомлень, що використовують функції хешування із ключем
61. CBC-MAC
62. Поняття про цифровий підпис (на прикладі RSA та Ель-Гамаля), вимоги до нього
63. Основні алгоритми електронного цифрового підпису, DSA
64. Стандарти ЕЦП Р 34.10 та Р 34.10-2001
65. Український алгоритм ЕЦП ДСТУ 4145
66. Стеганографічні системи. Модель та основні вимоги.
67. Відкриті, закриті та напівзакриті стеганосистеми.
68. Атаки на стеганографічні системи та протидія їм.
69. Пропускна здатність каналів приховуваної передачі повідомлень.
70. Оцінювання стійкості стеганографічних систем.
71. Методи стеганографії. Текстова стеганографія.
72. Методи стеганографії. Цифрова стеганографія.

73. Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіо файлах.
74. Цифрові водяні знаки.
75. Методи модифікації найменшого значущого біта.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

13 Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет, робота з презентаціями.

Вивчення навчальної дисципліни не потребує використання спеціального програмного прикладного забезпечення, крім загальновживаних програм і операційних систем.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Історія криптології та секретного зв'язку/ Гребенніков В. В. Київ: Вид. «КНТ», 2023. 800 с.
2. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. Основи криптології: навч. посібник/ Щур Н.О., Покотило О.А. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

Додаткова

1. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.
2. Криптологія: навч. посібник/ М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
3. Криптологія у прикладах, тестах і задачах: навч. посібник/ Т.В. Бабенко, Г.М. Гулак, С.О. Сушко, Л.Я. Фомичова. Д.: Національний гірничий університет, 2013. 318 с.
4. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

ПРИКЛАДНА КРИПТОЛОГІЯ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Четвертий, п'ятий
Кількість встановлених кредитів ЄКТС	9
Форми навчання, для яких викладається дисципліна	Очна денна

Результати навчання. Студент, який успішно завершив вивчення дисципліни, повинен: *застосовувати* теорії та методи криптографічного захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах; *вирішувати* задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах, з використанням сучасних методів та засобів криптографічного захисту інформації; *виконувати* впровадження та підтримку компонентів криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах; *адаптуватися* в умовах частої зміни технологій професійної діяльності та *прогнозувати* кінцевий результат при вирішенні практичних задач криптографічного захисту інформації.

Зміст навчальної дисципліни. Введення в криптологію. Класичні шифри. Потокові та блочні симетричні шифри. Міжнародні стандарти блокового симетричного шифрування. Вітчизняні криптографічні стандарти. Стійкі та нестійкі генератори псевдовипадкових чисел. Асиметричні криптографічні системи шифрування. Елементи криптоаналізу. Основи теорії автентичності. Криптографічні хеш-функції. Цифрові підписи. Стеганографія.

Пререквізити – математичні основи захисту інформації; теорія інформації та кодування.

Кореквізити – проєктно-технологічна практика; компонентна база і схемотехніка систем захисту.

Запланована навчальна діяльність: лекції – 32 год., лабораторні роботи – 68 год., самостійна робота – 170 год.; разом – 270 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, тестування, підсумковий контрольний захід.

Вид семестрового контролю: іспит, іспит.

Навчальні ресурси:

1. Історія криптології та секретного зв'язку/ Гребенніков В. В. Київ: Вид. «КНТ», 2023. 800 с.
2. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. Основи криптології: навч. посібник/ Щур Н.О., Покотило О.А. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
5. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
6. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

Викладач: Анікін В. А.