ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету IT
Підпис Олег САВЕНКО Ім'я, ПРІЗВИЩЕ
«08» 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптологія

Галузь знань	12 – Інформаційні технології
Спеціальність	125 – Кібербезпека
Рівень вищої освіти	Перший бакалаврський
Освітньо-професійна програма	Кібербезпека
Обсяг дисципліни	9 кредитів ЄКТС
Шифр дисципліни	ОПП.05
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		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
Очна (денна)	2	3	9	270	102	34	51	17		168		+		+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доц. Віра ТІТОВА
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

ПРИКЛАДНА КРИПТОЛОГІЯ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Третій
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 стандарти блокового симетричного шифрування. Генератори псевдовипадкових чисел. Асиметричні криптографічні системи шифрування. Елементи криптоаналізу. Основи теорії автентичності. Криптографічні хеш-функції. Цифрові підписи. Стеганографія.

Пререквізити – теорія ймовірності та математична статистика; теорія інформації та кодування.

Кореквізити – технічний і криптографічний захист інформації; компонентна база і схемотехніка систем захисту.

Запланована навчальна діяльність: лекції – 34 год., лабораторні роботи – 51 год., практичні заняття – 17 год., самостійна робота – 168 год.; разом – 270 год.

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

Форми оцінювання результатів навчання: захист лабораторних робіт, виконання практичних завдань, письмова контрольна робота, захист курсової роботи, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; 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. Прикладна криптологія: системи шифрування: підручник/ О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. К.: ДУТ, 2014. 448 с.
3. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
4. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 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: к.т.н., доцент Тітова В.Ю.

ВСТУП

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

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; 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 магістрів зі спеціальності «Кібербезпека та захист інформації»:

***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.

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ФК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

результати навчання:

ПРН5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН47. 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.

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

Назва теми	**Кількість годин відведених на:**			
	лекції	**практичні заняття**	**лабораторні роботи**	**самостійну роботу**
Тема 1. Введення в криптологію	2	-	-	2
Тема 2. Класичні шифри	4	6	18	60
Тема 3. Симетричні криптосистеми	8	4	12	36
Тема 4. Асиметричні криптосистеми	4	-	9 (10/8)*	9 (8/10)*
Тема 5. Елементи криптоаналізу	4	2	6	36
Тема 6. Автентифікація та хешування	6	2	6	14
Тема 7. Цифрові підписи	2	3 (4/2)*	-	7 (6/8)*
Тема 8. Стеганографія	4	-	-	4
Разом:	**34**	**17 (18/16)***	**51 (52/50)***	**168 (166/170)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Введення в криптологію	
1	**Введення в криптологію** 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. [3] с. 14-36	2
	Тема 2. Класичні шифри	
2	**Класичні шифри (частина 1)** 1. Шифри простої заміни 2. Гомофонний шифр заміни 3. Поліграмні шифри 4. Поліалфавітні шифри [2] с. 131-140; [3] с. 42-89	2
3	**Класичні шифри (частина 2)** 1. Шифри перестановки 2. Багаторазове шифрування 3. Роторні шифрувальні машини 4. Афінні шифри. 5. Шифр гамування [2] с. 140-147; [3] с. 89-101	2
	Тема 3. Симетричні криптосистеми	
4	**Потокові та блочні симетричні шифри** 1. Потокові симетричні шифри (A5, RC4, STRUMOK). Синхронні та самосинхронізовані потокові шифри. 2. Блокові симетричні шифри (RC2, RC5, SAFER, FEAL, Blowfish, мережа Фейстеля). 3. Методи компонування сучасних блокових симетричних шифрів. [1] с. 47-60; [2] с. 147-158; [3] с. 101-127, 148-172	2
5	**Міжнародні стандарти блокового симетричного шифрування (частина 1)** 1. Стандарт DES. Структура алгоритму шифрування даних. Режими виконання алгоритму (електронна кодова книга, зчеплення блоків зашифрованих даних, зворотний зв'язок за шифрованими даними та виходом, лічильник, тощо). 2. Симетричний алгоритм IDEA. Структура алгоритму шифрування даних. Безпека та вразливість ключів. [2] с. 158-169; [3] с. 172-215, 228-264	2
6	**Міжнародні стандарти блокового симетричного шифрування (частина 2)** 1. Стандарт AES (Rijndael). Структура алгоритму та раундів. Алгоритм розгортання ключа для шифрування даних. Відмінності шифрування та розширування. [2] с. 171-179; [3] с. 310-370	2

7	**Вітчизняні стандарти блокового симетричного шифрування** 1. Стандарт ДСТУ 28147:2009. Шифрування даних у режимі простої заміни. Шифрування даних у режимі гамування та зі зворотним зв'язком. Шифрування даних у режимі утворення імітовставки. 2. Стандарт блокового симетричного шифрування ДСТУ 7624:2014 «Калина» [2] с. 169-171, 179-191; [3] с. 270-310	2
Тема 4. Асиметричні криптосистеми		
8	**Генератори псевдовипадкових чисел.** 1. Основні визначення випадкової послідовності та вимоги до них. 2. Методи і засоби перевірки на випадковість. 3. Конгруентні генератори псевдовипадкових чисел. 4. Генератор Фібоначі. 5. Генератор псевдовипадкових чисел на основі алгоритму BBS. 6. Генератори псевдовипадкових чисел на основі регістрів зсуву зі зворотним зв'язком [3] с. 138-148	2
9	**Асиметричні криптографічні системи шифрування** 1. Криптографічна система Діффі–Хеллмана 2. Криптографічна система RSA 2. Криптографічна система Ель-Гамаля [3] с. 386-418	2
Тема 5. Елементи криптоаналізу		
10	**Елементи криптоаналізу (частина 1)** 1. Типи розкриття 2. Силові методи криптоаналізу 3. Криптоаналіз за побічними каналами 4. Криптоаналіз класичних шифрів. [2] с. 220-247; [4] с. 6-29, 46-50	2
11	**Елементи криптоаналізу (частина 2)** 1. Диференціальний криптографічний аналіз. 2. Лінійний криптографічний аналіз. 3. Властивості симетричності та вразливі ключі. 4. Атака "Квадрат". 5. Атака методом інтерполяцій. 6. Атака еквівалентних ключів. 7. Методи зламу на дискретному логарифмуванні. 8. Метод "крок немовляти, крок велетня". [3] с. 127-135, 215-228, 264-270, 370-386, 418-430	2
Тема 6. Автентифікація та хешування		
12	**Основи теорії автентичності** 1. Ідентифікація та автентифікація об'єктів 2. Задачі автентифікації у криптографічному захисті інформації 3. Парольна автентифікація. Методи формування стійких паролів 4. Поняття безумовно безпечних кодів автентифікації, теорія Симонсона. [2] с. 272-284	2
13	**Криптографічні хеш-функції (частина 1)** 1. Алгоритм MD5 2. Алгоритм SHA 3. Алгоритм SHA3	2

	4. Застосування функції хешування в криптографії [2] с. 284-296	
14	**Криптографічні хеш-функції (частина 2)** 1. Хеш-функції, що використовують симетричні блокові алгоритми 2. Функція хешування "Купина" – національний стандарт України ДСТУ 7564:2014 3. Коди автентифікації повідомлень, що використовують функції хешування із ключем 4. CBC-MAC [2] с. 296-308	2
Тема 7. Цифрові підписи		
15	**Цифрові підписи** 1. Поняття про цифровий підпис (на прикладі RSA та Ель-Гамаля), вимоги до нього 2. Основні алгоритми електронного цифрового підпису, DSA 3. Стандарти ЕЦП Р 34.10 та Р 34.10-2001 4. Український алгоритм ЕЦП ДСТУ 4145 [1] с. 117-129	2
Тема 8. Стеганографія		
16	**Стеганографія (частина 1)** 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. [2] с. 251-260	2
17	**Стеганографія (частина 2)** 1. Методи стеганографії. Текстова стеганографія. 2. Цифрова стеганографія. Приховування даних у нерухомих цифрових зображеннях, відеофайлах та аудіо файлах. 3. Цифрові водяні знаки. 4. Методи модифікації найменшого значущого біта. [2] с. 260-272	2
	Разом за семестр:	**34**

Зміст лабораторних робіт

№ п/п	**Теми лабораторних робіт**	**Кількість годин**
1	Перевірка стійкості шифрів стовпцевої та подвійної перестановки	6
2	Перевірка стійкості шифрів простої заміни та Цезаря	6
3	Перевірка стійкості шифрів Віженера та XOR	6
4	Шифрування даних у відповідності до стандартів DES та 3DES	6
5	Шифрування даних у відповідності до стандарту AES	6
6	Методи формування паролів та перевірки їх на стійкість	6
7	Розмежування повноважень на основі хешованої парольної аутентифікації	6
8	Шифрування даних у відповідності до стандарту RSA	6
9	Підсумкове заняття. Контрольна робота	3 (4/2)*
	Разом за семестр:	**51(52/50)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Зміст практичних занять

№ п/п	Теми практичних занять	Кількість годин
1	Шифри стандартної та подвійної перестановки	2
2	Шифри простої заміни та Цезаря	2
3	Шифри Віженера та XOR (шифр одноразового блокнота)	2
4	Алгоритм роботи DES та 3DES	2
5	Алгоритм роботи AES	2
6	Оцінювання стійкості паролів	2
7	Хеш-функції MD5 та SHA-1	2
8	Цифровий підпис RSA	2 (2/1)*
9	Підсумкове заняття.	1 (2/1)*
	Разом за семестр:	**17 (18/16)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни становить 168 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, підготовку до виконання та захисту лабораторних робіт, підготовку до практичних занять, роботу над курсовою роботою. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи (І семестр)	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1. Виконання завдань практичного заняття №1. Робота над КР відповідно до календарного плану.	10/10*
2	Опрацювання теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №1. Робота над КР відповідно до календарного плану.	10/10*
3	Опрацювання теоретичного матеріалу лекції №3. Виконання завдань практичного заняття №2. Робота над КР відповідно до календарного плану.	10/10*
4	Опрацювання теоретичного матеріалу лекції №4. Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2. Робота над КР відповідно до календарного плану.	10/10*
5	Опрацювання теоретичного матеріалу лекції №5. Виконання завдань практичного заняття №3. Робота над КР відповідно до календарного плану.	10/10*
6	Опрацювання теоретичного матеріалу лекції №6. Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3. Робота над КР відповідно до календарного плану.	10/10*
7	Опрацювання теоретичного матеріалу лекції №7. Виконання завдань практичного заняття №4. Робота над КР відповідно до календарного плану.	10/10*
8	Опрацювання теоретичного матеріалу лекції №8. Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4. Робота над КР відповідно до календарного плану.	10/10*
9	Опрацювання теоретичного матеріалу лекції №9. Виконання завдань практичного заняття №5. Робота над КР відповідно до календарного плану.	10/10*
10	Опрацювання теоретичного матеріалу лекції №10. Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5. Робота над КР відповідно до календарного плану.	10/10*
11	Опрацювання теоретичного матеріалу лекції №11. Виконання завдань практичного заняття №6. Робота над КР відповідно до календарного плану.	10/10*
12	Опрацювання теоретичного матеріалу лекції №12. Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6. Робота над КР відповідно до календарного плану.	10/10*
13	Опрацювання теоретичного матеріалу лекції №13. Виконання завдань практичного заняття №7. Робота над КР відповідно до календарного плану.	10/10*

14	Опрацювання теоретичного матеріалу лекції №14. Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7. Робота над КР відповідно до календарного плану.	10/10*
15	Опрацювання теоретичного матеріалу лекції №15. Виконання завдань практичного заняття №8. Робота над КР відповідно до календарного плану.	10/10*
16	Опрацювання теоретичного матеріалу лекції №16. Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8. Підготовка до захисту КР.	8/10*
17	Опрацювання теоретичного матеріалу лекції №17. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом. Підготовка до захисту КР.	8/10*
	Разом за семестр:	168 (166/170)*

* При плануванні лекцій за чисельником/за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

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.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: обговорення проблемних питань під час лекцій, прилюдні захисти лабораторних робіт з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт і контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок визнання та перезарахування результатів навчання здобувачів вищої освіти у ХНУ.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- захист лабораторних робіт;
- виконання практичних завдань;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Оцінювання курсового проєктування. Навчальним планом дисципліни передбачено курсовий проєкт під керівництвом викладача та з консультуванням за графіком. Згідно з навчальним планом підготовки бакалаврів за спеціальністю «Кібербезпека» курсовий проєкт виконується у 3 семестрі поетапно, відповідно до календарного плану.

Календарний план виконання курсової роботи:

Зміст етапу	Термін виконання
1. Огляд предметної області, збирання теоретичного матеріалу	1-7 тиждень
2. Розробка криптографічної системи згідно завдання	8-9 тиждень
3. Криптоаналіз розробленої системи	10-11 тиждень
4. Написання тексту пояснювальної записки та розробка графічних матеріалів. Оформлення курсової роботи, як документа, відповідно до вимог.	12-13 тиждень
5. Здача курсової роботи на попередню перевірку. За необхідності корегування, доповнення і виправлення пояснювальної записки згідно зауважень керівника.	14-15 тиждень
6. Захист курсової роботи.	16-17 тиждень

Завдання на курсову роботу базується на матеріалі, який опрацьовується під час лекційних, лабораторних, практичних занять та самостійної роботи в ході вивчення дисципліни, а також на основі практичних навичок та компетентностей, набутих студентом в ході вивчення попередніх та супутніх дисциплін. Тематика курсової роботи пов'язана з майбутньою спеціальністю ЗВО. Орієнтовна тематика завдань є наступною:

1. Розробити доказово-стійку криптографічну систему для захисту довільної текстової інформації. Систему реалізувати на основі комбінації трьох методів підстановки, використавши два з числа тих, що були розглянуті на лабораторних роботах №1-4, та один з розділу «класичні шифри» середовища CrypTool, які не були розглянуті.

2. Перевірити стійкість системи за допомогою інструментів криптоаналізу.

3. Систему побудувати у середовищі CrypTool, перевірку організувати за допомогою інструментарію даного ж середовища.

Пояснювальна записка повинна бути обсягом 18-25 сторінок.

Варіанти завдань до курсової роботи

№ варіанту	**Види шифрів, які комбінуються**
1	Заміни + Віженера + ADFGVX
2	Заміни + Віженера + Chaocipher
3	Заміни + Подвійна перестановка + LAMBDA1
4	Заміни + Віженера + Josse-Cipher
5	Заміни + Віженера + LAMBDA1
6	Заміни + Подвійна перестановка + ADFGVX
7	Заміни + Віженера + M209
8	Заміни + Подвійна перестановка + M209
9	Заміни + Віженера + T-310
10	Заміни + Віженера + Вернама
11	Подвійна перестановка + Цезаря + Playfair
12	Подвійна перестановка + Цезаря + Іспанський шифр
13	Подвійна перестановка + Цезаря + M-138
14	Подвійна перестановка + Цезаря + Solitaire
15	Подвійна перестановка + Цезаря + SIGABA
16	Подвійна перестановка + Цезаря + Purple
17	Подвійна перестановка + Цезаря + Сцитала
18	Подвійна перестановка + Цезаря + Straddling Checkerboard
19	Подвійна перестановка + Цезаря + XOR
20	Подвійна перестановка + Цезаря + Enigma
21	Звичайна перестановка + Віженера + Straddling Checkerboard

22	Звичайна перестановка + Віженера + Вернама
23	Звичайна перестановка + Віженера + Хілла
24	Звичайна перестановка + Віженера + Enigma
25	Звичайна перестановка + Віженера + Solitaire
26	Звичайна перестановка + Віженера + XOR
27	Звичайна перестановка + Віженера + Сцитала
28	Звичайна перестановка + Віженера + ADFGVX
29	Звичайна перестановка + Віженера + Іспанський шифр
30	Звичайна перестановка + Віженера + Playfair

Структурування курсової роботи за етапами і оцінювання результатів навчання ЗВО за ваговими коефіцієнтами

1 етап	2 етап	3 етап	4 етап	5 етап	Захист КР
ВК:0,1	ВК:0,1	ВК:0,1	ВК:0,1	ВК:0,1	ВК:0,5

При оцінюванні курсової робота враховується дотримання в ній ряду вимог. Виконання курсової роботи передбачає ґрунтовне вивчення літературних джерел з обраної теми, теоретичні знання та практичні навички, аналізу напрацьованих міжнародних практик (стандартів, методологій), власне творче бачення ЗВО, своєчасність виконання кожного етапу у відповідності до календарного плану. При проведенні захисту та оцінюванні курсової роботи використовуються такі критерії.

Оцінка «відмінно» виставляється, якщо: курсова робота виконана в повному обсязі відповідно до завдань, робота демонструє творчий підхід, технічно досконала. У пояснювальній записці теоретичний матеріал подано послідовно, грамотно використано спеціальну термінологію. Результат виконаної роботи повністю відповідає чинним якісним та кількісним показникам або може бути кращий від них. Під час захисту на всі запитання дано вичерпну відповідь.

Оцінка «добре» виставляється, якщо: ЗВО виконав поставлені завдання на належному рівні та показав володіння системними професійними знаннями в повному обсязі. Робота виконана з врахуванням встановлених вимог, демонструє творчий підхід, але має незначні технічні недоліки. Під час захисту у відповідях можливі 1-2 неточності в термінології і другорядних висновках.

Оцінка «задовільно» виставляється, якщо: ЗВО при виконанні курсової роботи на різних етапах припускався помилок і неточностей, які виправляв після консультації з керівником. Робота має окремі недоліки, але в цілому має завершений вигляд. Під час захисту ЗВО на частину поставлених запитань не дав відповіді, або ж відповіді були не повні.

Оцінка «незадовільно» виставляється, якщо курсова робота виконана не у повному обсязі та з відхиленням від визначеної тематики. Робота не відповідає встановленим вимогам, містить грубі помилки, під час захисту ЗВО не дав відповіді на більшість поставлених запитань. Така курсова робота потребує переробки.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота		**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Практичні заняття	Контрольна робота	Семестровий контроль (іспит)
Тема	1-8		1-8	1-8
Ваговий коефіцієнт	0,2	0,2	0,2	0,4

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення презентації виконаного завдання; вільне володіння студентом спеціальною термінологією і уміння застосовувати знання на практиці; своєчасна здача завдання з практики. Оскільки виконане завдання з практики є допуском до виконання відповідної за темою та номером лабораторної роботи, то термін здачі практики вважається своєчасним, якщо студент здав її в день виконання відповідної лабораторної роботи або до цього моменту. У випадку невиконання практики студент не допускається до виконання відповідної за темою та номером лабораторної роботи та зобов'язаний здати виконане практичне завдання у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі. Оцінку за практичне заняття викладач оголошує одразу після здачі і проставляє в електронний журнал дисципліни.

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: оцінка, отримана за здачу відповідної за номером та темою практики; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи. Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. 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.

Оцінювання контрольних робіт. Контрольна робота складається з двох теоретичних питань та однієї задачі за темами практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичні питання та правильно вирішив задачу.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичні питання та правильно вирішив задачу, але у відповіді присутні дві-три несуттєві помилки.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичні питання або припустився помилок при вирішення задачі.

Оцінку «незадовільно» отримує студент, який не дав відповіді на теоретичні питання або не зміг вирішити задачу.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з двох теоретичних питань і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	**Узагальнений критерій**
Відмінно	Студент 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 державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, 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 закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент 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 студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, 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	Студент 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 студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з

дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
A	4,75–5,00	5	***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	***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 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.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Технології захисту інформації/ Ю. А. Тарнавський. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.
2. 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.
3. Прикладна криптологія: системи шифрування: підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. К.: ДУТ, 2014. 448 с.
4. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.

Додаткова

5. Криптологія: навч. посібник/ М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. К.: Видавничий дім «Кондор», 2020. 248 с.
6. Основи криптології: навч. посібник/ Щур Н.О., Покотило О.А. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
7. 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.
8. Історія криптології та секретного зв'язку/ Гребенніков В. В. Київ: Вид. «КНТ», 2023. 800 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