Силабус курсу
Криптографія

Ступінь вищої освіти – бакалавр
Освітня програма «Кібербезпека»

Дні занять: _____, _____, ауд. ____; _____, _____, ауд. ____
Консультації: _____ _____, ауд. ____

Рік навчання: III,**Семестр:** V

Кількість кредитів: 5 **Мова викладання:** українська

Керівник курсу

ПІП д.т.н., професор, професор кафедри кібербезпеки **Михайло КАСЯНЧУК**

Контактна інформація kmm@wunu.edu.ua, +38 (0352) 47 50 50 *6501

Опис дисципліни

Метою дисципліни "Криптографія" є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного криптографічного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів криптографічного захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Структура курсу

Години (лек. / сем.)	Тема	Результати навчання	**Завдання**
2 / 2	**Тема 1.** Вступ. Шифри перестановки та простої заміни.	Вступ. Задачі криптографії. Основні поняття та положення комп'ютерної криптографії. Принципи криптографічного захисту інформації. Криптоаналітичні атаки. Їх види. Шифр скитала. Шифруючі таблиці. Шифр магічних квадратів. Шифр Кардано. Шифр атбаш. Полібіанський квадрат. Шифр Цезаря. Шифр Цезаря з ключовим словом. Шифруючі таблиці Трисемуса.	Тести, задачі, питання
2 / 2	**Тема 2.** Шифри складної заміни. Шифр одноразового блокноту.	Шифр Гронсфельда. Шифр Гронсфельда з ключовим словом. Шифр Віженера. Шифр Віженера з ключовим словом. Роторні шифрувальні машини. Роторна шифрувальна машина Enigma. Біграмний шифр Плейфейра. Подвійний квадрат Уїтстона. Шифр чотирьох квадратів. Шифр ADFGVX. Шифр одноразового блокноту.	Тести, задачі, питання
2 / 2	**Тема 3.** Алгоритм DES.	Структура алгоритму DES. Його переваги та недоліки. Операції алгоритму DES. Функція шифрування алгоритму DES. Генерація підключів алгоритму DES. Режими роботи алгоритму DES: електронна кодова книга, зчеплення блоків шифру, зворотній зв'язок по шифртексту, зворотній зв'язок	Тести, задачі, питання

		по виходу. Галузі застосування алгоритму DES.	
2 / 2	**Тема 4.** Алгоритми IDEA та ГОСТ28147–89.	Структура алгоритму IDEA. Його переваги та недоліки. Операції алгоритму IDEA. Генерація підключів алгоритму IDEA. Загальна структура алгоритму ГОСТ28147–89. Його переваги та недоліки. Операції алгоритму ГОСТ28147–89. Генерація підключів алгоритму IDEA. Режими роботи алгоритму ГОСТ28147–89: проста заміна, гамування, гамування із зворотним зв'язком, вироблення імітовставки. Галузі застосування алгоритмів IDEA та ГОСТ28147–89.	Тести, задачі, питання
2 / 2	**Тема 5.** Український та світовий стандарти симетричного шифрування.	Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES (Rijndeal).	Тести, задачі, питання
2 / 2	**Тема 6.** Сімейство алгоритмів RC.	RC-подібні алгоритми. Алгоритми RC 2, RC 4, RC 5, RC 6.	Тести, задачі, питання
2 / 2	**Тема 7.** Арифметика асиметричних криптосистем.	Основні поняття. Алгоритм Евкліда, його наслідок, пошук оберненого елемента, китайська теорема про остачі. Функція Ейлера. Теореми Ейлера та Ферма.	Тести, задачі, питання
2 / 2	**Тема 8.** Криптосистема RSA.	Опис криптосистеми RSA. Генерування ключів. Шифрування та розшифрування. Коректність, ефективність та надійність криптосистеми.	Тести, задачі, питання
2 / 2	**Тема 9.** Криптосистема Рабіна.	Генерування ключів криптосистеми Рабіна. Шифрування та розшифрування в криптосистемі Рабіна. Коректність, ефективність та надійність криптосистеми.	Тести, задачі, питання
2 / 2	**Тема 10.** Криптосистема Ель–Гамаля.	Криптосистема Ель–Гамаля. Шифрування та розшифрування в криптосистемі Ель–Гамаля. Коректність, ефективність та надійність криптосистеми.	Тести, задачі, питання
2 / 2	**Тема 11.** Електронний цифровий підпис.	Поняття електронного цифрового підпису. Електронний цифровий підпис в системах RSA та Ель–Гамаля. Алгоритм DSA. Система Шнорра. Ефективність, достовірність та конфіденційність підписів у різних алгоритмах.	Тести, задачі, питання
2 / 2	**Тема 12.** Шифрування із паролем.	Шифрування із паролем. Апаратні пристрої збереження ключів. Криптографічні акселератори. Біометрична ідентифікація.	Тести, задачі, питання
2 / 2	**Тема 13.** Поняття хеш-функції. Застосування хеш-функцій.	Визначення функції хешування та вимоги до неї. Алгоритм функції хешування по ГОСТ Р 34.11-94. Аналіз алгоритму та особливостей його програмної реалізації. Геш-функції на основі ділення. Мультиплікативна схема гешування. Гешування	Тести, задачі, питання

		рядків змінної довжини. Криптографічні хеш-функції. Геометричне гешування. Прискорення пошуку даних.	
2 / 2	**Тема 14.** Хеш-функції типу MD та SHA. Український стандарт хешування.	Хеш-функція MD (MD-2, MD-4, MD-5). Сімейство хеш-функцій SHA (SHA-1, SHA-2, SHA-3, SHA-256). Український стандарт хешування ДСТУ 7564:2014 «Купина».	Тести, задачі, питання
2 / 2	**Тема 15.** Генерація ЕЦП на основі хеш-функцій.	Процедура вироблення та перевірки електронного підпису по ДСТУ 4145-2002. Генерація загальних параметрів, секретного та відкритого ключів. Особливості програмної реалізації процедури. Алгоритм DSA.	Тести, задачі, питання
2 / 2	**Тема 16.** Поняття еліптичної криптографії. Реалізація шифрування на еліптичних кривих.	Еліптичні криві над кінцевими полями. Еліптичні криві над полями непарної характеристики. Теорема Хассе. Еліптичні криві над полями характеристики 2. Проективні координати. Швидка редукція (NIST-криві). Еліптичні криві, рекомендовані NIST. Розмір ключа.	Тести, задачі, питання
2 / 2	**Тема 17.** ЕЦП на основі еліптичних кривих.	Особливості ЕЦП на основі еліптичних кривих. Вибір параметрів. Генерування ключів ECDSA. Переваги ECDSA перед DSA. Практична реалізація	Тести, задачі, питання
2 / 2	**Тема 18.** Криптографічні протоколи.	Визначення криптографічного протоколу. Перелік вимог до криптографічного протоколу. Аналіз атак на криптографічні протоколи. Використання симетричного та несиметричного шифрування в криптографічних протоколах.	Тести, задачі, питання
2 / 2	**Тема 19.** Приклади сучасних комп'ютерних криптографічних систем.	Характеристики протоколу SSL компанії Netscape Communication Corporation для захисту інформаційного обміну в середовищі Інтернет. Ієрархія ключів, блок-схема розсилки ключів абонентам мережі, блок-схема забезпечення цифрового підпису даних в мережі.	Тести, задачі, питання
2 / 2	**Тема 20.** Елементи стеганографії.	Комп'ютерна стеганографія. Методи вкладення інформації у файли мультимедіа. Методи приховування інформації в зображеннях. Методи приховування інформації в аудіо сигналах.	Тести, задачі, питання
2 / 2	**Тема 21.** Квантова криптографія.	Поняття квантової криптографії. Квантовий розподіл ключів. Способи та пристрої генерації та передачі одиночних фотонів. Фазове та часове кодування. Основні напрямки розвитку та проблеми квантової криптографії. Порівняльний аналіз протоколів квантової криптографії.	Тести, задачі, питання

Літературні джерела

1. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
2. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

3. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
4. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
5. 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.
6. Криптоаналіз. Криптографічні протоколи. Навчальний посібник/ О.М. Гапак. Ужгород: Ужгородський національний університет, 2021. 93 с.
7. Efficient coding for secure computing with additively-homomorphic encrypted data/ Thijs Veugen. - International Journal of Applied Cryptography, 2020, Vol.4, No.1. pp.1-15. DOI: 10.1504/IJACT.2020.107160/
8. Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». Тернопіль. 2020. 380 с.
9. Асиметричні алгоритми шифрування у системі залишкових класів / Я.М. Николайчук, І.З. Якименко, Н.Я. Возна, М.М. Касянчук // Кібернетика і системний аналіз, №4, Т.58. 2022. С. 129-138.
10. Symmetric Cryptoalgorithms in the Residue Number System/ Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko// Cybernetics and Systems Analysis. Springer US, is. 52, 2021. PP. 219-223.
11. Cryptology and information security - past, present, and future role in society/ S. Bhattacharya. International Journal on Cryptography and Information Security (IJCIS). Vol. 9, No.1/2, 2019. P. 13-36.
12. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків/ І.З. Якименко, Л.М. Тимошенко, М.М. Касянчук. Сучасна спеціальна техніка, №2, 2018. С.63-71.
13. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ М. М. Касянчук, М. П. Карпінський, С. В. Казмірчук. Захист інформації, №2, т.21, 2019. С.65-73.
14. Розробка трьохмодульної криптосистеми Рабіна на основі операції додавання/ М.М. Касянчук, О.Я. Лотоцький, С.В. Яцків, С.В. Івасьєв, Л.М. Тимошенко. Informatics & Mathematical Methods in Simulation, №11, 2021. С. 47-57.

Політика оцінювання

- **Політика щодо дедлайнів та перескладання**: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).
- **Політика щодо академічної доброчесності**: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).
- **Політика щодо відвідування**: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

Оцінювання

Остаточна оцінка за курс розраховується наступним чином:

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на лабораторних заняттях: 11 тем по 2 бали – max 22 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання: Захист 11 лабораторних робіт по 2 бали – max 22 балів.	1. Усне опитування на лабораторинх заняттях: 10 тем по 2 бали – max 20 балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання: Захист 10 лабораторних робіт по 3 бали – max 30 бали.	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Виконання завдань на тренінгах – max 30 балів	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання студентів:

ECTS	Бали	Зміст
A	90-100	відмінно
B	85-89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов’язковим повторним курсом