Назва курсу	**«Шифрування та безпека даних»**
Викладач (-і)	Касянчук Михайло Миколайович
Профайл викладача (-ів)	http://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	kmm@wunu.edu.ua

Анотація до курсу.

Даний курс знайомить студентів із основними фундаментальними поняттями і законами криптографії для їх використання в сучасних кіберсистемах; принципами побудови криптографічних алгоритмів, основними криптографічними стандартами та їх використання в задачах захисту інформації; основним математичним апаратом та законами криптографії у професійній діяльності; програмними та апаратними засобами, які реалізують основні криптографічні алгоритми для вирішення типових задач захисту інформації.

Мета та цілі курсу.

Мета курсу "Шифрування та безпека даних" полягає у формуванні 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.

Загальна інформація про дисципліну

Ступінь вищої освіти	**бакалавр**
Спеціальність	**124 – Системний аналіз**
Курс (рік навчання)	**3**
Семестр	**6**
Нормативна \ вибіркова	**Вибіркова**
Загальна кількість год кредитів	**5**

Перелік тем

Тема 1. Вступ. Основні поняття та визначення. Законодавство України в галузі захисту інформації. Принципи криптографічного захисту інформації.

Тема 2. Класичні симетричні криптосистеми.

Тема 3. Сучасні симетричні криптосистеми. Алгоритм DES.

Тема 4. Сучасні симетричні криптосистеми. Алгоритм IDEA, стандарт шифрування ГОСТ 28147–89. Сімейство алгоритмів RC.

Тема 5. Арифметика асиметричних криптосистем. Афінні шифри.

Тема 6. Криптосистема RSA.

Тема 7. Криптосистеми Рабіна та Ель–Гамаля.

Тема 8. Електронний цифровий підпис.

Тема 9. Криптографічні протоколи.

Тема 10. Проблема ідентифікації та аутентифікації користувача. Парольна та

біометрична ідентифікація.

Тема 11. Особливості фізичного, технічного та програмного захисту інформації.

Тема 12. Віруси. Захист інформації від вірусів. Основні антивірусні програми.

Тема 13. Безпека сучасних мережевих технологій, методи і засоби захисту від віддалених атак через Інтернет.

Тема 14. Захист інформації в електронних платіжних системах (ЕПС).

Рекомендовані джерела інформації

Основна література

1. Wong David. Real-World Cryptography. Manning Publications, 2020. — 350 p.
2. Cryptography with Coding Theory. 3rd Edition. — Pearson Education, 2020. — 977 p.
3. Stallings William. Cryptography and Network Security: Principles and Practice. 8th Edition. — Pearson Education, 2020. — 1513 p.
4. Ryabko Boris. Cryptography In The Information Society. World Scientific Publishing, 2021. — 286 p.

Додаткова література

5. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. 3rd edition. — New York: CRC Press/Taylor & Francis Group, 2021. — 649 p.
6. Alginahi Y.M., Kabir M.N. (eds.) Authentication Technologies for Cloud Computing, IoT and Big Data. The Institution of Engineering and Technology, 2019. — 370 p.
7. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.
8. Yan B., Xiang Y., Hua G. Improving Image Quality in Visual Cryptography. Springer, 2020. — 131 p.

Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Шифрування та безпека даних» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2		Модуль 3	Модуль 4
20%	20%	20%	20%	5%	15%
Поточне оцінювання	Модульний контроль	Поточне оцінювання	Модульний контроль	Тренінг	Самостійна робота
Середнє арифметичне з оцінок, отриманих на заняттях по темах 1-7	Оцінка за модульну контрольну роботу	Середнє арифметичне з оцінок, отриманих на заняттях по темах 8-14	Оцінка за модульну контрольну роботу	Оцінка за виконання тренінгу	Оцінка за виконання самостійної роботи

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовольняє, може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)

85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

Навчальні ресурси

№	Найменування
1.	**Обладнання:** проектор, комп'ютери з доступом до мережі Інтернет.
2.	Програмне забезпечення: VSCode, PyCharm, Visual Studio 2015, Visual Studio™ 2015, Visual Studio Team System 2015.

Політики курсу.

Академічна доброчесність. **Дотримання академічної доброчесності студентами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.