Назва курсу	**«Захист інформації»**
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**
Сторінка курсу в moodle	https://moodle.wunu.edu.ua
Консультації	вівторок: 13-00, ауд. 6501. Онлайн- консультації: у Telegram-групі курсу або ZOOM кожного дня з 14 -00 до 18-00.

1. Анотація до курсу.

Даний курс знайомить студентів із основними фундаментальними поняттями, законами і теоріями для ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

2. Мета та цілі курсу.

Мета курсу "Захист інформації" полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Результати навчання:

- засвоїти основні фундаментальні поняття і закони стосовно захисту інформації для їх використання в сучасних комп'ютерних системах;
- отримати теоретичні знання, вміння та навики для вибору системи захисту інформації та її реалізації;
- отримати практичні навики використання сучасних технологій захисту інформації
- знати принципи побудови криптоалгоритмів, їх основних стандартів та використання в задачах захисту інформації;
- вміти використовувати програмні та апаратні засоби, які реалізують основні функції захисту інформації.

Загальна інформація про дисципліну

Ступінь вищої освіти	**бакалавр**
Галузь знань	**02 Культура і мистецтво**
Спеціальність	**028 «Менеджмент соціокультурної діяльності»**
Освітньо-професійна програма	**«Менеджмент соціокультурної діяльності»**
Курс (рік навчання)	**четвертий**
Семестр	**7**
Нормативна \ вибіркова	**Вибіркова**
Загальна кількість год/кредитів	**150/5**
Лекції, год.	**26**
Практичні, год	**13**

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.

Тема 4. Арифметика асиметричних криптосистем. Афінні шифри.

Тема 5. Криптосистема RSA.

Тема 6. Криптосистеми Рабіна та Ель–Гамаля.

Тема 7. Електронний цифровий підпис.

Тема 8. Криптографічні протоколи.

Тема 9. Проблема ідентифікації та аутентифікації користувача. Парольна та біометрична ідентифікація.

Тема 10. Особливості фізичного, технічного та програмного захисту інформації.

Тема 11. Віруси. Захист інформації від вірусів. Основні антивірусні програми.

Тема 12. Безпека сучасних мережевих технологій, методи і засоби захисту від віддалених атак через Інтернет.

Тема 13. Захист інформації в електронних платіжних системах (ЕПС).

Рекомендовані джерела інформації

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.

15. Симетрична система з нелінійним шифруванням та можливістю контролю шифротексту з метою маскування/ В.М. Джулій, І.В. Муляр, В.С. Орленко, В.Ю. Тітова, В.А. Анікін// Вісник Хмельницького національного університету. Технічні науки. 2020. № 6. С. 33-39

Система оцінювання та вимоги.

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

Заліковий модуль 1 - 30%

Заліковий модуль 2 (підсумкова контрольна робота) – 40%

Заліковий модуль 3 (оцінка за КПІЗ, враховуючи поточне опитування) - 30%

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:

Підсумковий бал	**Оцінка за традиційною шкалою**
	залік
90-100	зараховано
89-70	
60-69	
26-59	не зараховано
1-25	

6. 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.
3.	Електронний варіант лекцій
4.	Методичні вказівки до виконання практичних робіт (електронний варіант)

7. 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.