Назва курсу	**«Захист інформації»**
Викладач	Касянчук Михайло Миколайович
Профайл викладача	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	**029 Інформаційна, бібліотечна та архівна справа**
Освітньо-професійна програма	**«Документознавство та інформаційна діяльність»**
Курс (рік навчання)	**другий**
Семестр	**4**
Нормативна \ вибіркова	**Вибіркова**
Загальна кількість год/кредитів	**150/5**

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.

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.

Оцінювання Модуль 1	**Модуль 2**	**Модуль 3**	
40%	40%	5%	15%
Поточне оцінювання Оцінка за поточне опитування визначається як середнє арифметичне з оцінок, отриманих під час практичних занять	*Модульний контроль* Підсумкова письмова робота.	*Тренінг* Оцінка за тренінг визначається як середнє арифметичне з оцінок, отриманих під час виконання завдань тренінгу	*Самостійна робота* Оцінка за самостійну роботу визначається як середнє арифметичне оцінок, отриманих за виконання завдань самостійної роботи блоку 1 і 2.

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.

Політика щодо дедлайнів і перескладання. Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Використання друкованих і електронних джерел інформації під час контрольних заходів та екзаменів заборонено.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу з дозволу дирекції факультету.